Steffen Kionke, Eduard Schesler

Modul 61117

Gruppentheorie

LESEPROBE

Fakultät für
Mathematik und Informatik

FernUniversität in Hagen

Inhaltsverzeichnis

Einleitung und Studierhinweise

Einleitung

Gruppen begegnen einem im Studium der Mathematik oder Informatik relativ früh. Wahrscheinlich kennen Sie schon die additive Gruppe eines Vektorraumes und die symmetrische Gruppe aller Permutationen der Zahlen $\{1, 2, \ldots, n\}$. Vielleicht kennen Sie auch schon die algebraische Definition von Gruppen:

Eine Gruppe ist eine Menge G mit einer assoziativen Multiplikation $*\colon G \times G \to G$, sodass G ein neutrales Element enthält und zu jedem Element in G auch ein Inverses bezüglich der Multiplikation existiert.

Diese Definition vergisst man dann schnell wieder, weil der Begriff der Gruppe insgesamt etwas zu unscheinbar ist. Und in der Tat trifft man zwar in vielen Bereichen auf spezielle Beispiele von Gruppen, zur Theorie der Gruppen erfährt man aber wenig. Das Ziel dieses Kurses ist es das zu ändern. Wir werden die Theorie der Gruppen von Grund auf entwickeln und ich hoffe, Sie dadurch überzeugen zu können, dass Gruppen unvorstellbar vielfältige Objekte sind.

Man darf dabei nicht vergessen, dass die abstrakte Definition von Gruppen, wie sie heute verwendet wird, natürlich nicht vom Himmel gefallen ist. Sie hat sich aus verschiedenen Beobachtungen herausgebildet. Anders ausgedrückt: Gruppen kommen „natürlich" in der Mathematik (und in der Natur) vor, allerdings braucht Zeit um das abstrakte Konzept dahinter zu begreifen.

Die Anfänge der Gruppentheorie liegen im Studium der Permutationsgruppen, also von Untergruppen der symmetrischen Gruppe. Es ist nicht verwunderlich, dass sich Menschen in verschiedensten Bereichen Gedanken über mögliche Vertauschungen bestimmter Objekte gemacht haben. Ein frühes Beispiel ist das *Wechselläuten*, das im 15. Jahrhundert in England aufkam. Dabei möchte man eine gewisse Anzahl an Kirchenglocken wiederholt läuten, diese aber bei jedem „Wechsel“ in einer anderen Reihenfolge erklingen lassen. Wenn man nun noch zusätzliche Bedingungen an die Wechsel stellt, stößt man schnell auf nicht-triviale Fragen über die symmetrische Gruppe. In der Mathematik taucht die Idee der Gruppe zuerst im Zusammenhang mit der Frage nach der Auflösbarkeit polynomieller Gleichungen auf. Galois[1] ist der erste der erkennt, dass man die Auflösbarkeit einer polynomiellen Gleichung anhand einer „Gruppe“ von Permutationen ihrer Lösungen entscheiden kann. Diese Einsicht ist heute als *Hauptsatz der Galoistheorie* bekannt (dieses Ergebnis lernt man im Kurs „Algebra“). Gruppen von Permutationen wurden unter anderem von Camille Jordan[2] weiter untersucht. Die abstrakte Idee der Gruppe taucht aber wahrscheinlich das erste Mal in den Arbeiten von Arthur Cayley[3] auf.

Einen weiteren Schub erhält die Gruppentheorie dann 1872 durch das *Erlangener Programm* von Felix Klein[4]. Klein schlägt vor Geometrien mithilfe von Gruppen zu klassifizieren. Die zentrale Einsicht dabei ist, dass die „Symmetrien“ eines geometrischen Objektes eine Gruppe bilden und, dass diese Gruppe schon das Wesen des geometrischen Objektes kennt. Dieser Standpunkt hat sich etabliert und prägt bis heute unsere Sicht auf Gruppen. Er führt zur verbreiteten Volksweisheit

> Man versteht eine Gruppe am besten, indem man sie als Symmetriegruppe eines geeigneten Objektes identifiziert.

Heute würde man sagen, dass man die Gruppe „wirken“ lässt.

Danach hat sich die Gruppentheorie rasant entwickelt und viele verschiedenen Teilgebiete ausgebildet. Lange Zeit bildeten die endlichen Gruppen einen Schwerpunkt dieser Untersuchungen. Aber spätestens mit der vollständigen Klassifikation der endlichen einfachen Gruppen in den 1980er Jahren nahm auch das Interesse an unendlichen Gruppen stark zu. Vor allem der Einsatz

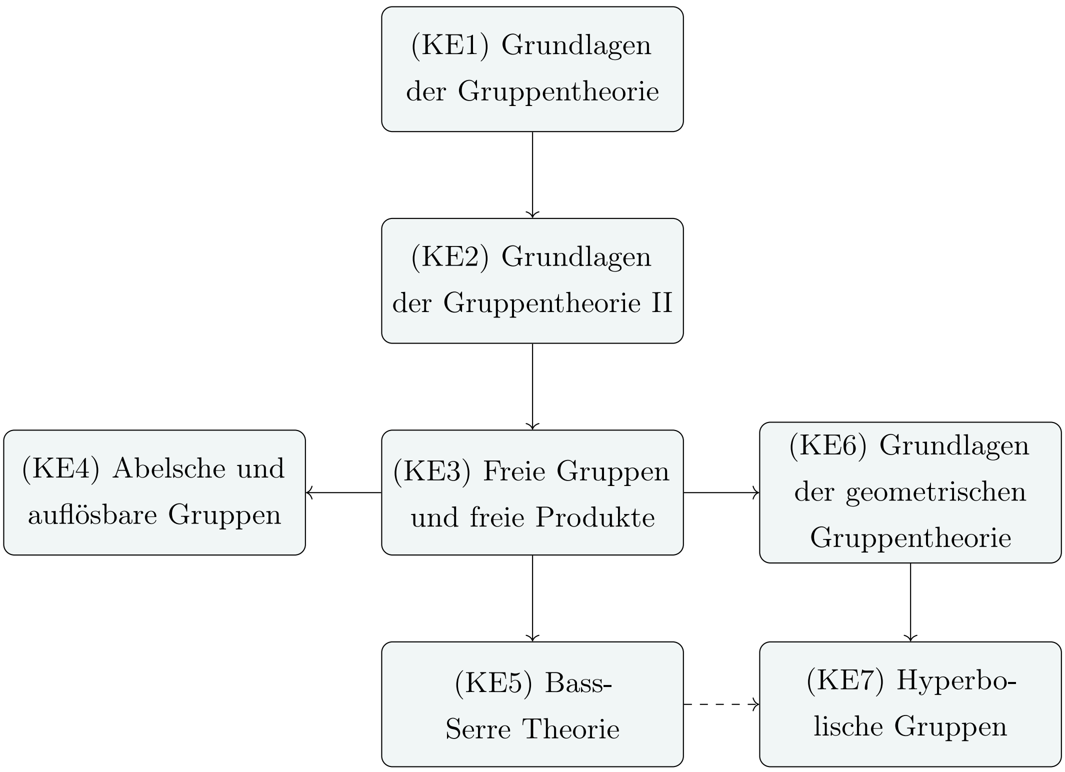
---

[1] Évariste Galois: französischer Mathematiker, 1811–1832. Stirbt im Alter von 20 Jahren bei einem Duell.
[2] Camille Jordan: französischer Mathematiker, 1838–1922.
[3] Arthur Cayley: britischer Mathematiker, 1821 – 1895.
[4] Felix Klein: deutscher Mathematiker, 1849 – 1925.

geometrischer Methoden hat zu vielen neuen Entwicklungen geführt, die man heute unter dem Namen *geometrische Gruppentheorie* kennt.

In diesem Kurs werden wir uns von den Grundlagen der Gruppentheorie bis zu den Anfängen der geometrischen Gruppentheorie vorarbeiten. Unser Fokus liegt dabei eher auf den unendlichen Gruppen. Das große Thema „endliche Gruppen" streifen wir nur. Die klassischen Ergebnisse über endliche Gruppen werden stattdessen im Kurs „Algebra" behandelt.

In den ersten beiden Kurseinheiten behandeln wir die Grundlagen, die Sie auch in den meisten Büchern zur Algebra finden. In der dritten Kurseinheit besprechen wir freie Gruppen und freie Produkte. Dabei nehmen wir schon einen geometrischen Standpunkt ein. In der vierten Kurseinheit behandeln wir die abelschen und auflösbaren Gruppen, weil das in keinem Kurs über Gruppentheorie fehlen darf. In der fünften Kurseinheit diskutieren wir die Bass-Serre Theorie. In den letzten beiden Kurseinheiten sind wir dann bei den Grundlagen der geometrischen Gruppentheorie angekommen.



Allgemeine Studierhinweise

Die zwei wichtigsten Hinweise zum Studium der Mathematik kennen Sie natürlich schon aus anderen Kursen, trotzdem schadet es nicht sie nochmal zu wiederholen.

→ Machen Sie sich die Hände schmutzig: *Bearbeiten Sie Übungsaufgaben!* Das Nachprüfen von Einzelheiten, das selbstständige Rumprobieren und das Aufschreiben von Argumenten sind (leider!?) der einzige Weg, um mit den Konzepten wirklich vertraut zu werden.

→ Keine Scheu: *Stellen Sie Fragen!* Man muss nicht jede Nuss alleine knacken. Ob Sie die Kursbetreuer oder Ihre Kommilitonen fragen, ist dabei nebensächlich. Wichtig ist sich überhaupt auszutauschen. Oft lernt man schon durch das Formulieren einer Frage etwas dazu.

In der Moodle-Lernumgebung zum Kurs finden Sie übrigens ein Diskussionsforum und Zusatzmaterialien zum Kurs (Einsendeaufgaben, Tests zu Selbstkontrolle, Videos,...).

Eingangsvoraussetzungen

Dieser Kurs entwickelt die Gruppentheorie von Grund auf und es werden nur wenige Vorkenntnisse benötigt. In jedem Fall sind aber gute Kenntnisse der Module „Mathematische Grundlagen“ und „Lineare Algebra“ wichtig. Ab Kurseinheit 6 werden auch Begriffe aus dem Kurs „Analysis“ verwendet (vor allem stetige Abbildungen, offene Menge). Da dieser Kurs auf dem Niveau des Masterstudiums angesiedelt ist, erfordert das Studium (insbesondere der Kurseinheiten 5, 6 und 7) eine gewisse Sicherheit im Umgang mit Mathematik.

Struktur des Lehrtextes

Der Kurstext besteht aus sieben Kurseinheiten und einem Anhang. Jede Kurseinheit beginnt mit Studierhinweisen bestehend aus Literaturangaben und einem Fahrplan durch die Kurseinheit. Die Unterabschnitte im Kurstext sind vollständig nummeriert (1.1.1, 1.1.2, ...) um das Fragestellen zu erleichtern. Die jeweils letzte Unterabschnittsnummer auf einer Seite findet man immer oben rechts in der Kopfzeile, sodass sie beim Blättern leicht zu den entsprechenden Stellen gelangen.

Der Kurstext enthält viele Übungsaufgaben, deren Lösungen Sie jeweils am Ende jeder Kurseinheit finden. Ein rotes „L“ am rechten Rand dient jeweils als Link zur Lösung der Aufgabe. **L**

Wichtige Sätze und Definitionen sind am linken Rand durch einen grauen Balken hervorgehoben.

Das „gefährliche Kurve“-Symbol von Bourbaki wird verwendet um auf mögliche Missverständnisse hinzuweisen.

Am Ende des Kurstextes finden Sie einen Index, ein Literaturverzeichnis und ein Symbolverzeichnis.

Notation

Die folgenden Symbole und Bezeichnungen werden im Kurstext verwendet. Im Kurs neu eingeführte Symbole und Schreibweisen findet man im Symbolverzeichnis.

$\mathbb{C}$	Die komplexen Zahlen.
$\mathbb{N}$	Die natürlichen Zahlen ohne Null $\{1, 2, 3, 4, \dots\}$.
$\mathbb{N}_0$	Die natürlichen Zahlen mit Null $\{0, 1, 2, 3, 4 \dots\}$.
$\mathbb{Q}$	Die rationalen Zahlen
$\mathbb{R}$	Die reellen Zahlen
$\mathbb{Z}$	Die ganzen Zahlen $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
$\mathbb{F}_p$	Der endliche Körper mit p Elementen.
$\mathrm{Abb}(X, Y)$	Die Menge aller Abbildungen $X \to Y$.
$\mathrm{ggT}(a, b)$	Der größte gemeinsame Teiler von $a, b \in \mathbb{N}$.
$\mathrm{kgV}(a, b)$	Das kleinste gemeinsame Vielfache von $a, b \in \mathbb{N}$.
$\Re(z), \Im(z)$	Real- und Imaginärteil der komplexen Zahl z.
$\subseteq$	Teilmenge.
$\bigcup$	Vereinigung.
$\bigsqcup$	disjunkte Vereinigung.

Auszug aus dem griechischen Alphabet

Steffen Kionke

Gruppentheorie

Kurseinheit 2:
Grundlagen der Gruppentheorie II

Fakultät für
Mathematik und Informatik

FernUniversität in Hagen

Studierhinweise zur zweiten Kurseinheit

In der zweiten Kurseinheit werden wir einige weitere Grundbegriffe der Gruppentheorie kennenlernen. Wir beginnen mit dem sehr wichtigen Konzept der Gruppenwirkungen. Grob gesagt, ist eine Gruppenwirkung eine Möglichkeit sich eine Gruppe als „Symmetriegruppe“ eines Objektes vorzustellen. Gruppenwirkungen sind in der Gruppentheorie allgegenwärtig und es ist wichtig, dass Sie mit diesem Begriff gut vertraut sind. Wir veranschaulichen die Nützlichkeit von Gruppenwirkungen in dieser Kurseinheit anhand von Beispielen in der abzählenden Kombinatorik. Im Weiteren besprechen wir einige fundamentale Konstruktionen der Gruppentheorie mit deren Hilfe wir viele neue Beispiele von Gruppen erhalten. Wir beginnen mit dem direkten Produkt von Gruppen und besprechen im Anschluss zwei Verallgemeinerungen: das semidirekte Produkt und das Faserprodukt. Dabei werden wir zu diesen Konstruktionen jeweils die zugehörige „universelle Eigenschaft“ kennenlernen. Die universelle Eigenschaft bietet einen guten Weg zum Verständnis dieser Konstruktionen und macht auch den Unterschied zwischen den Konstruktionen deutlich. Die Faserprodukte werden wir schließlich verwenden um alle Untergruppen des direkten Produktes zweier Gruppen zu beschreiben.

Lernziele

Nach dem Drucharbeiten der Kurseinheit sollten Sie

- → mit dem Begriff der *Gruppenwirkung* umgehen können und den *Bahn-Stabilisator*-Satz kennen,
- → die *Burnside'sche Formel* auf Probleme der abzählenden Kombinatork anwenden können,
- → *primitive* und *mehrfach transitive* Gruppenwirkungen verstehen,
- → das *direkte Produkt* und seine universelle Eigenschaft kennen,
- → das *semidirekte Produkt* und seine Eigenschaften kennen, sowie Beispiele von semidirekten Produkten nennen können,
- → das *Faserprodukt* und seine universelle Eigenschaft kennen

→ verstehen, wie man die Untergruppen des direkten Produktes zweier Gruppen mithilfe von Faserprodukten beschreiben kann.

Literaturhinweise

Gruppenwirkungen und die Konstruktion von direkten und semidirekten Produkte finden Sie wieder in sehr vielen einführenden Büchern zur Algebra oder Gruppentheorie. Zum Beispiel:

→ [Fis17]: Kapitel 1: 1.3.2 – 1.3.6 und 1.4, 1.5.1.

→ [JS14]: Kapitel I, §5, §6.

→ [Mac12]: Kapitel 2: 2.6, 2.7, und Kapitel 3: 3.1, 3.3.

→ [Rob95]: Kapitel I, 1.4 – 1.6.

→ [Rot95]: Kapitel 2 (direkte Produkte, S. 40), Kapitel 3, Kapitel 7 (semidirekte Produkte, S.167).

Primitive und mehrfach transitive Wirkungen finden Sie in den Büchern über Gruppentheorie von Robinson und Rotman

→ [Rob95]: Kapitel 7.

→ [Rot95]: Kapitel 9.

Faserprodukte sind in der Literatur nur schwer zu finden. Sie werden eher allgemein in der Sprache der Kategorientheorie als „pullback“ beschrieben (vgl. [Lan02, I. §11]). Die Beschreibung der Untergruppen von direkten Produkten durch Faserprodukte basiert auf einer Idee, die ich in einer Arbeit von Jaques Thévenaz [Thé97] gefunden habe.

Fahrplan durch die Kurseinheit

2.1 → Abschnitt 2.1 beginnt mit der Definition von *Gruppenwirkungen* (2.1.2) und einigen Anmerkungen dazu (2.1.3). Danach folgen mehrere Beispiele von Gruppenwirkungen (2.1.4–2.1.7) mit deren Hilfe man ein Gefühl für dieses Konzept entwickeln kann. Als erste Anwendung erhalten wir den klassischen Satz von Cayley (2.1.8). Im Anschluss besprechen wir die Begriffe *Bahn* (2.1.10), *Stabilisator*

(2.1.11) und *Fixpunkt* (2.1.14), die man unbedingt kennen muss um mit Gruppenwirkungen zu arbeiten. Ein wichtiges Ergebnis ist der *Bahn-Stabilisator-Satz* (2.1.19). Dieser Satz stellt einen Zusammenhang zwischen Bahn und Stabilisator her und sagt uns, dass alle transitiven Gruppenwirkungen so „aussehen“ wie in Beispiel 2.1.17. Als Anwendung besprechen wir die Bahnengleichung (2.1.21) und die Burnside'sche Formel (2.1.22). Mit der Burnside'schen Formel kann man viele schöne Beispiele in der abzählenden Kombinatorik untersuchen und ein Blick in die Literatur dazu lohnt sich. Wir diskutieren hier nur ein Beispiel (2.1.23).

2.2 → In Abschnitt 2.2 besprechen wir den Zusammenhang zwischen maximalen Untergruppen und primitiven Gruppenwirkungen; ein klassisches Beispiel dafür wie Gruppenwirkungen eingesetzt werden. Im ersten Teil definieren wir *maximale Untergruppen* (2.2.3), halten zwei Beobachtungen fest (2.2.4) und sehen uns Beispiele an (2.2.5–2.2.8). Im zweiten Teil des Abschnittes definieren wir dann *Blöcke* (2.2.10) und *primitive Wirkungen* (2.2.11). Anhand der Beispiele 2.2.13 und 2.2.14 kann man sich einen ersten Eindruck verschaffen. Im Hilfssatz 2.2.15 halten wir ein paar nützliche Tatsachen fest, die wir dann verwenden um den wichtigen Satz 2.2.17 zu beweisen, der den Zusammenhang zwischen maximalen Untergruppen und primitiven Wirkungen herstellt.

Den dritten Teil von 2.2 besprechen wir dann kurz das stärkere Konzept der mehrfach transitiven Gruppenwirkung (2.2.18). Ein wichtiges Ergebnis um diesen Begriff zu verstehen, ist das Kriterium für mehrfache Transitivität 2.2.22. Merken sollte man sich in jedem Fall, dass 2-transitive Wirkungen immer primitiv sind (2.2.23). Dies ermöglicht es weitere Beispiele von primitiven Wirkungen anzugeben.

2.3 → Abschnitt 2.3 enthält die Konstruktion des *direkten Produktes* einer Familie von Gruppen (2.3.2, 2.3.3). Um mit diesen Gruppen zu arbeiten, ist es hilfreich sich die universelle Eigenschaft (2.3.5) einzuprägen. Satz 2.3.7 bietet ein Kriterium um zu entscheiden, ob eine Gruppe das direkte Produkt zweier Normalteiler ist. Als Beispiel sehen wir uns an, wie sich zyklische Gruppen als direkte Produkte schreiben lassen (2.3.9, 2.3.10). Zum Vergleich besprechen wir auch eine verwandte Konstruktion: das *beschränkte direkte Produkt* (2.3.11 – 2.3.16). Diese Konstruktion ist weniger wichtig und es genügt, wenn Sie sich den Unterschied zum direkten Produkt bewusst machen.

2.4 → Abschnitt 2.4 erläutert das *semidirekte Produkt*. Eine Konstruktion, die in der Gruppentheorie sehr häufig auftaucht und die Sie sich sehr genau einprägen sollten. Der erste Teil beginnt mit *Wirkungen durch Automorphismen* (2.4.2), einigen Anmerkungen (2.4.3) und Beispielen (2.4.4, 2.4.5). Die Konstruktion des semidirekten Produktes besprechen wir in 2.4.6 und fassen die wichtigsten Eigenschaften im Satz über das semidirekte Produkt zusammen (2.4.7). Danach folgen Beispiele und Aufgaben zum semidirekten Produkt, die man sich auf jedem Fall anschauen sollte (2.4.8–2.4.13).

Im zweiten Teil des Abschnittes besprechen wir die universelle Eigenschaft des semidirekten Produktes (2.4.14) und verwenden diese um ein wichtiges Kriterium (2.4.17) herzuleiten, mit dem man zeigen kann, dass eine Gruppe ein semidirektes Produkt ist. Wir illustrieren das Kriterium anhand von zwei Beispielen (2.4.19, 2.4.20). Schließlich besprechen wir noch eine andere Sicht auf semidirekte Produkte: spaltende kurze exakte Folgen (2.4.21–2.4.24). Hier geht es vor allem darum, Sie mit dem Begriff der *kurzen exakten Folge* vertraut zu machen.

Der dritte Teil des Abschnittes enthält zum Abschluss ein schönes Beispiel eines semidirekten Produktes: die Isometriegruppe des $\mathbb{R}^n$ (2.4.25). Mit Satz 2.4.26 kann man die Isometriegruppe sehr gut verstehen.

2.5 → Abschnitt 2.5 beginnt mit der Konstruktion des *Faserproduktes* (2.5.2) und der universellen Eigenschaft (2.5.3) dazu. Jedes Faserprodukt ist eine Untergruppe eines direkten Produktes und der entscheidende Satz in diesem Abschnitt (2.5.5) besagt, dass man mithilfe von Faserprodukten wirklich alle Untergruppen des direkten Produktes zweier Gruppen beschreiben kann. In 2.5.6 besprechen wir kurz inwiefern diese Beschreibung sogar eindeutig ist. Als Anwendung überlegen wir uns wie man normale Untergruppen (2.5.9) und maximale Untergruppen (2.5.13) des direkten Produktes zweier Gruppen beschreiben kann.

2.1. Gruppenwirkungen

2.1.1 Wir haben bisher einen ersten Einblick in die Welt der Gruppen gewonnen und dabei vor allem erste Eigenschaften von Gruppen benannt. Was macht man aber mit Gruppen? Warum taucht dieses Konzept in der Mathematik so oft auf?

Gruppen beschreiben Symmetrieeigenschaften von mathematischen Objekten. Am deutlichsten haben wir das in der Aufgabe 1.2.5 gesehen, als wir die Symmetriegruppe des Quadrates bestimmt haben. Ein anderes Beispiel ist die symmetrische Gruppe S_n, die aus den „Symmetrien" (genauer: Bijektionen) der Menge $\{1, 2, \ldots, n\}$ besteht. Genauso könnte man die Automorphismengruppe $\mathrm{Aut}(G)$, als Gruppe der „Symmetrien" von G bezeichnen. Man merkt schon, dass das Wort „Symmetrie" hier sehr flexibel verwendet wird. Es bezeichnet im weitesten Sinne eine bijektive Selbstabbildung einer Menge, die eine vorgegebene Struktur erhält.

Nimmt man nun eine Gruppe G, dann stellt sich also die naheliegende Frage: *Die Symmetrien welcher Objekte beschreibt* G? Der springende Punkt ist natürlich, dass eine Gruppe auf vielen Arten als „Symmetrien" von verschiedensten Objekten aufgefasst werden kann. Man sagt in diesem Fall, dass G auf einem Objekt *wirkt*. Eine grundlegende Einsicht der Gruppentheorie ist nun, dass man Gruppen sehr gut mit Hilfe ihrer „Wirkungen" untersuchen kann.

2.1.2 **Definition**. Es sei G eine Gruppe und X eine Menge. Eine *Wirkung* von G auf X ist eine Abbildung

$$\cdot\colon G \times X \to X \quad \text{mit} \quad (g, x) \mapsto g \cdot x,$$

die den folgenden Eigenschaften genügt:

(W1) $e \cdot x = x$ für alle $x \in X$,

(W2) $g \cdot (h \cdot x) = (gh) \cdot x$ für alle $g, h \in G$ und $x \in X$.

2.1.3 **Anmerkungen zur Definition**.

(a) Gruppenwirkungen werden in der Literatur häufig mit anderen Begriffe bezeichnet. Einige Quellen verwenden die Bezeichnung „Gruppenoperation" (entlehnt aus dem Französischen „*opérations des groupes*“) oder „Gruppenaktion“ (entlehnt aus dem Englischen „*group action*“). Eine Menge X mit einer Wirkung der Gruppe G, bezeichnet man auch als *G-Menge*.

(b) Es sei X eine G-Menge. Für jedes feste $g \in G$, ist die Abbildung

$$\lambda_g \colon x \mapsto g \cdot x$$

eine Bijektion von X. In der Tat, die Abbildung $\lambda_{g^{-1}}$ ist die Umkehrabbildung, denn

$$g^{-1} \cdot (g \cdot x) = e \cdot x = x \quad \text{und} \quad g \cdot (g^{-1} \cdot x) = e \cdot x = x$$

für alle $x \in X$.

(c) Als direkte Folgerung aus (W2) erhalten wir die Identität

$$\lambda_g \circ \lambda_h = \lambda_{gh}$$

für alle $g, h \in G$. Das bedeutet, die Zuordnung $g \mapsto \lambda_g$ definiert einen Gruppenhomomorphismus $\lambda \colon G \to \mathrm{Sym}(X)$.

Sei nun umgekehrt $\alpha \colon G \to \mathrm{Sym}(X)$ ein Homomorphismus von G in die symmetrische Gruppe einer Menge X. Dann ist die Abbildung $\cdot_\alpha \colon G \times X \to X$ mit der Abbildungsvorschrift

$$(g, x) \mapsto g \cdot_\alpha x := \alpha(g)(x)$$

eine Wirkung von G auf X. Dabei impliziert die Gleichung $\alpha(e) = \mathrm{id}_X$ das Axiom (W1). Außerdem gilt (W2), denn

$$g \cdot_\alpha (h \cdot_\alpha x) = \alpha(g)(\alpha(h)(x)) = (\alpha(g) \circ \alpha(h))(x) = \alpha(gh)(x) = (gh) \cdot_\alpha x$$

für alle $g, h \in G$. Dies ergibt eine alternative Definition für Gruppenwirkungen: *Eine Wirkung von G auf X ist ein Homomorphismus $G \to \mathrm{Sym}(X)$.*

(d) Ist $H \leq G$ eine Untergruppe, so kann man eine Wirkung von G auf X zu einer Wirkung von H auf X einschränken. Die Axiome (W1) und (W2) bleiben offensichtlich richtig, auch wenn man nur Elemente der Untergruppe H einsetzen darf.

2.1.4 Beispiel. Es sei X eine Menge. Das mustergültige Beispiel einer Gruppenwirkung ist die Abbildung

$$\mathrm{Sym}(X) \times X \to X \quad \text{mit} \quad f \cdot x := f(x).$$

Es handelt sich um eine Wirkung von $\mathrm{Sym}(X)$ auf X, denn es gelten $\mathrm{id}(x) = x$ und

$$f \cdot (g \cdot x) = f(g(x)) = (f \circ g)(x) = (f \circ g) \cdot x$$

für alle $f, g \in \mathrm{Sym}(X)$ und alle $x \in X$. Der zugehörige Homomorphismus (siehe 2.1.3 (c)) $\mathrm{Sym}(X) \to \mathrm{Sym}(X)$ ist die identische Abbildung.

2.1.5 Beispiel. Es sei K ein Körper. Die Gruppe $\mathrm{GL}_n(K)$ wirkt auf der Menge K^n durch Matrix-Vektor-Multiplikation:

$$\mathrm{GL}_n(K) \times K^n \to K^n \quad \text{mit} \quad A \cdot v := Av.$$

Das ist leicht zu sehen, denn bekanntlich ist $E_n v = v$ und $A(Bv) = (AB)v$ für alle $v \in K^n$ und $A, B \in \mathrm{GL}_n(K)$.

2.1.6 Beispiel. Die Isometriegruppe $\mathrm{Isom}(\mathbb{R}^n)$ (siehe 1.1.13) wirkt auf $\mathbb{R}^n$ durch

$$f \cdot v := f(v).$$

Dabei handelt es sich um eine Einschränkung der Wirkung von $\mathrm{Sym}(\mathbb{R}^n)$ aus Beispiel 2.1.4 auf die Untergruppe $\mathrm{Isom}(\mathbb{R}^n)$. Durch dieselbe Vorschrift wirkt die Symmetriegruppe $\mathrm{Isom}(\mathbb{R}^n, M)$ einer Teilmenge $M \subseteq \mathbb{R}^n$ auf M.

2.1.7 Beispiel. Es sei G eine Gruppe. Dann wirkt G auf sich selbst durch *Linksmultiplikation*, d.h.,

$$g \cdot x := gx.$$

Das Wirkungsaxiom (W2) folgt dabei direkt aus dem Assoziativgesetz und das Axiom (W1) gilt, weil e das neutrale Element ist.

2.1.8 Satz (Cayley[1]). *Jede Gruppe G ist isomorph zu einer Untergruppe von* $\mathrm{Sym}(G)$.

Beweis. Wir betrachten die Wirkung von G auf sich selbst durch Linksmultiplikation; siehe 2.1.7. Die Linksmultiplikation mit $g \in G$ bezeichnen wir durch

[1] Arthur Cayley: englischer Mathematiker, 1821–1895.

$\lambda_g \colon G \to G$. Nach 2.1.3 (c) ist die Abbildung $\lambda \colon g \mapsto \lambda_g$ ein Gruppenhomomorphismus von G nach $\mathrm{Sym}(G)$. Der Kern von λ ist trivial, denn $\lambda_g(e) = g$. Also ist λ ein Isomorphismus auf sein Bild. □

2.1.9 **Aufgabe**. Wir betrachten die *obere Halbebene* $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ der komplexen Zahlen mit positivem Imaginärteil. Für $z \in \mathcal{H}$ und **L**

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

definieren wir

$$A \cdot z := \frac{az+b}{cz+d}.$$

Zeigen Sie, dass $A \cdot z$ definiert ist und in $\mathcal{H}$ liegt. Zeigen Sie weiter, dass dies eine Wirkung von $\mathrm{SL}_2(\mathbb{R})$ auf $\mathcal{H}$ definiert.

Die Selbstabbildung $z \mapsto A \cdot z$ der oberen Halbebene nennt man *Möbius-Transformation*[2]. Da die Matrix $-E_2$ trivial wirkt (also $-E_2 \cdot z = z$ für alle $z \in \mathcal{H}$), faktorisiert die Wirkung zu einer Wirkung der *projektiven speziellen linearen Gruppe* $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm E_2\}$.

2.1.10 **Die Bahn**. Es seien G eine Gruppe und X eine Menge mit G-Wirkung. Für $x \in X$ nennt man die Menge

$$G \cdot x := \{g \cdot x \mid g \in G\}$$

die *Bahn* von x. In manchen Texten wird auch die Bezeichnung *Orbit* verwendet.

Zwei Bahnen $G \cdot x$ und $G \cdot y$ sind entweder gleich oder disjunkt.
Das sieht man so: Ist $z = g \cdot x = h \cdot y$ in beiden Bahnen, so gilt für alle $g' \in G$ auch

$$g' \cdot x = g' \cdot (g^{-1} g \cdot x) = g' g^{-1} \cdot (h \cdot y) = g' g^{-1} h \cdot y.$$

Das heißt, die Bahn $G \cdot x$ ist in der Bahn $G \cdot y$ enthalten. Durch Vertauschen der Rollen von x und y folgt $G \cdot x = G \cdot y$.

[2]August Ferdinand Möbius: deutscher Mathematiker, 1790–1868.

Die Beziehung „in derselben Bahn liegen“ ist eine Äquivalenzrelation auf X deren Äquivalenzklassen genau die Bahnen sind. Die Menge der Bahnen heißt auch der *Bahnenraum* und wird mit X/G bezeichnet.

Die Wirkung heißt *transitiv*, wenn es nur eine Bahn gibt. In anderen Worten, wenn $G \cdot x = X$ für ein (und dann alle) $x \in X$ gilt.

2.1.11 Der Stabilisator. Es seien G eine Gruppe, X eine G-Menge und $x \in X$. Die Menge

$$\mathrm{St}_G(x) \coloneqq \{g \in G \mid g \cdot x = x\}$$

heißt der *Stabilisator* von x in G.

Der Stabilisator ist eine Untergruppe von G. Offensichtlich ist $e \in \mathrm{St}_G(x)$ und für $g, h \in \mathrm{St}_G(x)$ gilt $gh^{-1} \in \mathrm{St}_G(x)$, denn

$$gh^{-1} \cdot x = gh^{-1} \cdot (h \cdot x) = gh^{-1}h \cdot x = g \cdot x = x.$$

Man nennt die Wirkung von G auf X *frei*, wenn alle Stabiliatoren trivial sind, d.h., $\mathrm{St}_G(x) = \{e\}$ für alle $x \in X$.

2.1.12 Beispiel (Konjugation). Jede Gruppe G wirkt auf sich mittels *Konjugation*

$$(g, x) \mapsto {}^g x,$$

d.h., $g \in G$ wirkt durch den inneren Automorphisms ι_g; siehe 1.1.20. Zwei Elemente $x, y \in G$ liegen genau dann in derselben Bahn, wenn sie im Sinne von 1.1.21 konjugiert sind. Die Bahnen sind also genau die *Konjugationsklassen.* Den Stabilisator von $x \in G$ nennt man den *Zentralisator* von x und wir bezeichnen ihn mit

$$Z_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Der Zentralisator besteht genau aus den Elementen von G, die mit x vertauschen.

2.1.13 Definition. Es seien G eine Gruppe und $T \subseteq G$ eine Teilmenge. Die Untergruppe

$$Z_G(T) \coloneqq \{g \in G \mid gtg^{-1} = t \ \text{ für alle } t \in T\}$$

heißt der *Zentralisator von T in G*. (Um zu sehen, dass dies eine Untergruppe ist, kann man 1.2.7 verwenden, denn $Z_G(T) = \bigcap_{t \in T} Z_G(t)$.)

2.1.14 **Fixpunkte**. Es sei wieder X eine G-Menge. Für jedes $g \in G$ definieren wir die Menge der *Fixpunkte* von g als

$$\mathrm{Fix}_X(g) = \{x \in X \mid g \cdot x = x\}.$$

Diese Elemente werden also von g nicht bewegt.

2.1.15 **Beispiel** (Konjugation von Untergruppen). Es sei G eine Gruppe und $\mathcal{U}$ die Menge aller Untergruppen von G. Dann wirkt G durch Konjugation auf $\mathcal{U}$, d.h.,

$$(g, H) \mapsto {}^gH.$$

Den Stabilisator $\mathrm{St}_G(H)$ von $H \leq G$ unter der Konjugationswirkung nennt man den *Normalisator* von H in G:

$$N_G(H) \coloneqq \{g \in G \mid {}^gH = H\}.$$

Die Fixpunkte der Konjugationswirkung auf den Untergruppen sind genau die Normalteiler; siehe 1.2.24.

2.1.16 **Hilfssatz**. *Es sei X eine G-Menge. Für alle $x \in X$ und $g \in G$ gilt*

$$\mathrm{St}_G(g \cdot x) = g \,\mathrm{St}_G(x) g^{-1}.$$

Insbesondere haben Elemente in derselben Bahn konjugierte Stabilisatoren.

<u>*Beweis*</u>. Für alle $h \in \mathrm{St}_G(x)$ gilt

$$(ghg^{-1}) \cdot (g \cdot x) = gh \cdot x = g \cdot (h \cdot x) = g \cdot x$$

und daraus folgt $g \,\mathrm{St}_G(x) g^{-1} \subseteq \mathrm{St}_G(g \cdot x)$. Die umgekehrte Inklusion ist auch erfüllt, denn

$$\mathrm{St}_G(g \cdot x) = gg^{-1} \,\mathrm{St}_G(g \cdot x) gg^{-1} \subseteq g \,\mathrm{St}_G(g^{-1} \cdot (g \cdot x)) g^{-1} = g \,\mathrm{St}_G(x) g^{-1}. \quad \square$$

2.1.17 Beispiel (Wirkung auf G/H). Wir wollen Beispiel 2.1.7 etwas verallgemeinern. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann wirkt G auf der Menge der Linksnebenklassen G/H durch Linksmultiplikation, d.h.,

$$g \cdot xH := gxH.$$

Dies ist eine wohldefinierte Abbildung, denn falls x und y dieselbe Linksnebenklasse repräsentieren, dann gilt $y = xh$ für ein $h \in H$ und damit repräsentieren auch $gy = gxh$ und gx dieselbe Nebenklasse von H; vgl. 1.2.18 (a). Die Wirkungsaxiome folgen wieder unmittelbar aus den Gruppenaxiomen. Die Wirkung von G auf G/H ist transitiv, denn $G \cdot eH = G/H$. Aus 2.1.16 schließt man nun

$$\mathrm{St}_G(xH) = xHx^{-1},$$

denn der Stabilisator $\mathrm{St}_G(H)$ ist offenbar H.

2.1.18 Definition (Äquivarianz). Eine Abbildung $f\colon X \to Y$ zwischen G-Mengen X und Y heißt *äquivariant*, wenn

$$f(g \cdot x) = g \cdot f(x)$$

für alle $x \in X$ und $g \in G$ gilt. Gibt es eine bijektive, äquivariante Abbildung zwischen X und Y, dann sagen wir die G-Mengen seien *äquivalent*.

2.1.19 Bahn-Stabilisator-Satz. *Es sei X eine G-Menge. Für jedes $x \in X$ induziert die Bahnabbildung $B_x\colon g \mapsto g \cdot x$ eine bijektive, äquivariante Abbildung*

$$G/\,\mathrm{St}_G(x) \longrightarrow G \cdot x.$$

Sind G und X endlich, dann gilt

$$|G| = |G \cdot x|\,|\,\mathrm{St}_G(x)|.$$

Beweis. Wir beginnen mit einer Beobachtung: Ist $s \in \mathrm{St}_G(x)$, dann gilt $gs \cdot x = g \cdot (s \cdot x) = g \cdot x$ für alle $g \in G$. Das heißt, das Bild $B_x(g)$ von g unter der

Bahnabbildung, hängt nur von der Linksnebenklasse $g\,\mathrm{St}_G(x)$ ab. Damit ist die Abbildung

$$\widetilde{B}_x\colon G/\mathrm{St}_G(x) \to G\cdot x \quad \text{mit} \quad g\,\mathrm{St}_G(x) \mapsto g\cdot x$$

wohldefiniert. Es handelt sich um eine äquivariante Abbildung, denn

$$\widetilde{B}_x(gg'\,\mathrm{St}_G(x)) = gg'\cdot x = g\cdot(g'\cdot x) = g\cdot \widetilde{B}_x(g'\,\mathrm{St}_G(x)).$$

Nach Definition der Bahn ist die Abbildung sicherlich surjektiv. Wir müssen also noch prüfen, ob die Abbildung auch injektiv ist. Angenommen es gilt $\widetilde{B}_x(g\,\mathrm{St}_g(x)) = \widetilde{B}_x(h\,\mathrm{St}_G(x))$, also $g\cdot x = h\cdot x$. Dann ist $h^{-1}g\cdot x = x$ und damit liegt $h^{-1}g$ im Stabilisator $\mathrm{St}_G(x)$. Die Nebenklassen $h\,\mathrm{St}_G(x)$ und $g\,\mathrm{St}_G(x)$ sind also gleich.

Sind G und X endlich, dann folgt $|G/\mathrm{St}_G(x)| = \frac{|G|}{|\mathrm{St}_G(x)|}$ aus dem Satz von Lagrange 1.2.21 und mit der obigen Bijektion erhalten wir die Gleichung

$$|G| = |G\cdot x|\,|\mathrm{St}_G(x)|. \qquad \square$$

2.1.20 Eine wichtige Folgerung aus 2.1.19: *Jede transitive G-Wirkung ist äquivalent zu einer Linksmultiplikationswirkung auf Nebenklassen.* Das Beispiel in 2.1.17 beschreibt also (bis auf Äquivalenz) alle transitiven G-Wirkungen.

2.1.21 **Bahnengleichung**. Es sei G eine Gruppe und X eine endliche G-Menge. Ist $x_1, x_2, \ldots, x_k$ ein Vertretersystem für die Bahnen, dann gilt

$$|X| = \sum_{i=1}^{k} |G : \mathrm{St}_G(x_i)|.$$

Beweis. Wegen 2.1.10 ist X die disjunkte Vereinigung aller Bahnen. Weil $x_1, x_2, \ldots x_k$ ein Vertretersystem ist, gilt also

$$X = \bigsqcup_{i=1}^{k} G\cdot x_i$$

und aus 2.1.19 folgt

$$|X| = \sum_{i=1}^{k} |G \cdot x_i| = \sum_{i=1}^{k} |G : \mathrm{St}_G(x_i)|. \qquad \square$$

Das folgende Resultat geht auf Frobenius[3] zurück [Fro87]. Es wird aber in der Literatur oft als *Lemma von Burnside*[4] oder *Burnside'sche Formel* bezeichnet.

2.1.22 **Burnside'sche Formel.** *Es seien G eine endliche Gruppe und X eine endliche Menge mit G-Wirkung. Dann gilt*

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_X(g)| = |X/G|.$$

Beweis. Der Beweis verwendet die *Methode des doppelten Abzählens*. Bei dieser Methode wird eine Menge auf zwei verschiedene Weisen gezählt um eine Gleichung herzuleiten.

Es sei $P = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Für ein Paar $(g, x) \in G \times X$ sind also äquivalent:

$$(g, x) \in P \quad \Leftrightarrow \quad g \in \mathrm{St}_G(x) \quad \Leftrightarrow \quad x \in \operatorname{Fix}_X(g).$$

Dann gilt einerseits

$$|P| = \sum_{g \in G} \operatorname{Fix}_X(g)$$

und andererseits gilt

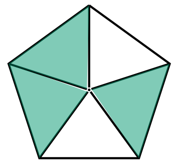
$$\frac{|P|}{|G|} = \frac{1}{|G|} \sum_{x \in X} |\mathrm{St}_G(x)| = \sum_{x \in X} |G : \mathrm{St}_G(x)|^{-1} = \sum_{x \in X} |G \cdot x|^{-1} = |X/G|. \qquad \square$$

2.1.23 **Beispiel.** Die Bahnengleichung und die Burnside'sche Formel sind in der

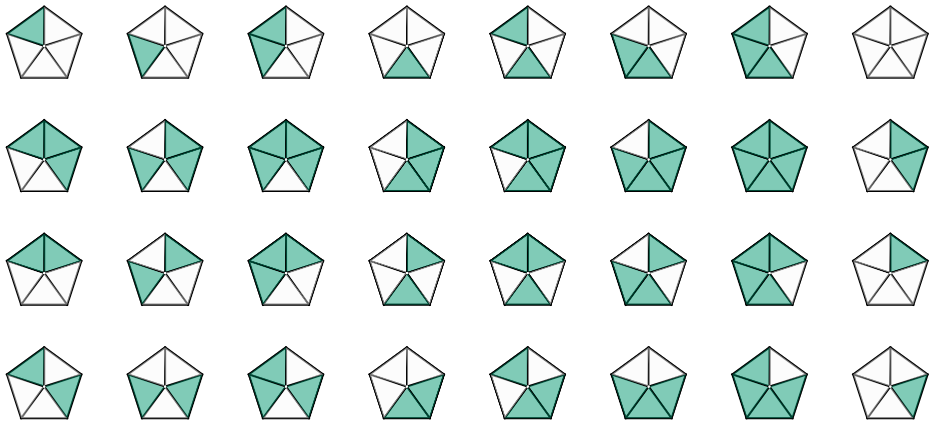
[3] Ferdinand Georg Frobenius: deutscher Mathematiker, 1849 – 1917.
[4] Willian Burnside: englischer Mathematiker, 1852 – 1927.

abzählenden Kombinatorik nützliche Hilfsmittel. Wir wollen das an einem einfachen Beispiel erläutern.

Fünfeckige Untersetzer sollen auf der Oberseite gefärbt werden. Dabei teilt man das Fünfeck in fünf gleiche Dreiecke ein, die jeweils weiß oder grün gefärbt werden sollen. Wieviele verschiedene Färbungen solcher Untersetzer gibt es?



Zunächst scheint es $2^5 = 32$ Möglichkeiten zu geben, den Untersetzer mit weiß und grün zu färben. Allerdings lassen sich manche der gefärbten Untersetzer durch eine Drehung ineinander überführen. Wir müssen also diese Symmetrien berücksichtigen.

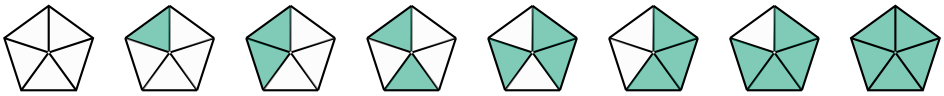


Dazu lassen wir eine zyklische Gruppe $G = \langle g \rangle$ der Ordnung 5 durch Drehungen auf der Menge der 32 gefärbten Fünfecke wirken. Zwei Fünfecke liegen in einer Bahn, wenn sie sich durch Drehung ineinander überführen lassen. Was wir eigentlich zählen wollen, ist die Anzahl der Bahnen!

Dazu benutzen wir die Burnside'sche Formel 2.1.22. Das neutrale Element e fixiert alle Fünfecke; es hat also 32 Fixpunkte. Alle anderen Elemente erzeugen G (siehe 1.5.7). Wenn ein gefärbtes Fünfeck Fixpunkt von $h \neq e$ ist, dann ist es also ein Fixpunkt von allen Gruppenelementen. Nur zwei Fünfecke haben den Stabilisator G: das vollständig weiße und das vollständig grüne. Die Burnside'sche Formel liefert uns nun

$$|X/G| = \frac{1}{5}(32 + 2 + 2 + 2 + 2) = \frac{40}{5} = 8.$$

Es gibt also insgesamt 8 echt verschiedene Untersetzer.



2.1.24 Aufgabe. Wir betrachten den Würfel $W = [-1,1]^3 \subseteq \mathbb{R}^3$. Die *Drehgruppe* von W ist die Gruppe **L**

$$D(W) = \{f \in \mathrm{SO}(3) \mid f(W) = W\}$$

aller Drehungen, die den Würfel erhalten.

(1) Bestimmen Sie die Ordnung $|D(W)|$ mithilfe der Bahnengleichung.

(2) Die Seitenflächen des Würfels sollen schwarz oder weiß gefärbt werden. Wieviele verschiedene Färbungen gibt es, wenn man durch Drehung ineinander überführbare Färbungen als gleich auffasst?

2.2. Primitive Wirkungen und maximale Untergruppen

2.2.1 Will man eine Gruppe verstehen, dann ist es ein erster naheliegender Ansatz sich zunächst einen (groben) Überblick über die auftretenden Untergruppen zu verschaffen. Dabei sind Untergruppen, die auffällige Eigenschaften aufweisen besonders relevant. Zum Beispiel könnte man fragen: Welches sind die „größten“ Untergruppen? So gelangt man zum Konzept der *maximalen Untergruppen*, das wir hier betrachten wollen. Wir werden insbesondere sehen, dass man maximale Untergruppen gut mithilfe von Gruppenwirkungen und dem Begriff der *primitiven* Wirkung beschreiben kann.

I. Maximale Untergruppen

2.2.2 Es sei G eine Gruppe. Eine Untergruppe $H \leq G$ heißt *echte* Untergruppe, wenn $H \neq G$ gilt.

2.2.3 **Definition** (maximale Untergruppe). Es sei G eine Gruppe und $M \leq G$ eine echte Untergruppe. Man nennt M eine *maximale Untergruppe* von G, wenn für jede Untergruppe $K \leq G$ mit $M \subsetneq K$ schon $K = G$ gilt.

2.2.4 **Anmerkungen zur Definition**.

(a) *Eine echte Untergruppe $M \lneq G$ ist genau dann maximal, wenn $\langle M \cup \{g\} \rangle = G$ für alle $g \in G \setminus M$ gilt.*

Falls M maximal ist, dann ist $M \subsetneq K = \langle M \cup \{g\} \rangle$ und damit $K = G$. Falls umgekehrt M nicht maximal ist, dann finden wir eine Untergruppe $M \lneq K \lneq G$ und für $k \in K \setminus M$ gilt dann $M \subsetneq \langle M \cup \{k\} \rangle \subseteq K \subsetneq G$.

(b) Jede endliche Gruppe besitzt maximale Untergruppen. Genauer gilt: Jede echte Untergruppe $H \subsetneq G$ einer endlichen Gruppe, ist in einer maximalen Untergruppe enthalten. In der Tat, dazu nimmt man einfach eine echte Untergruppe von G, die H enthält und dabei die größte Ordnung aller solcher Untergruppen aufweist.

2.2.5 **Beispiel**. Wir betrachten die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ der Ordnung n. Aus 1.5.1 wissen wir, dass es für jeden Teiler d von n genau eine Untergruppe der Ordnung

d in $\mathbb{Z}/n\mathbb{Z}$ gibt. Da alle diese Gruppen zyklisch sind, ist dabei die Gruppe der Ordnung d' genau dann in der Gruppe der Ordnung d enthalten, wenn gilt $d'|d$. Die Gruppe der Ordnung d ist also genau dann maximal, falls $p = n/d$ eine Primzahl ist. Mithilfe von Beispiel 1.2.3 kann man diese Untergruppen in der Form $p\mathbb{Z}/n\mathbb{Z}$ schreiben.

Etwas allgemeiner gilt:

2.2.6 **Hilfssatz**. *Es sei G eine Gruppe. Jede Untergruppe $M \leq G$, deren Index $|G : M|$ eine Primzahl ist, ist maximal.*

Beweis. Es sei $M \lneq K$ eine größere Untergruppe. Nach dem Indexsatz 1.2.20 gilt

$$|G : M| = |G : K| \cdot |K : M|$$

Da $|G : M|$ eine Primzahl ist und $|K : M| \neq 1$ gilt, folgt daraus $|G : K| = 1$ und somit $G = K$. □

2.2.7 **Aufgabe**. Wir betrachten die symmetrische Gruppe S_n. Zeigen Sie, dass **L**

$$M = \{\sigma \in S_n \mid \sigma(n) = n\}$$

eine maximale Untergruppe von S_n ist.

2.2.8 **Beispiel** ($\mathbb{Q}$ hat keine maximalen Untergruppen). Nicht jede Gruppe besitzt maximale Untergruppen. Als Beispiel wollen wir zeigen, dass die additive Gruppe $\mathbb{Q}$ keine maximale Untergruppe besitzt.

Es sei $H \lneq G$ eine echte Untergruppe. Wir wollen zeigen, dass H nicht maximal ist, indem wir eine größere Gruppe $K \lneq G$ konstruieren. Die Gruppe $H = \{0\}$ ist sicher nicht maximal, daher können wir $H \neq \{0\}$ annehmen. Also enthält H mindestens eine Zahl $\frac{a}{b} \neq 0$ mit $a, b \in \mathbb{N}$ und damit auch alle Vielfachen von $\frac{a}{b}$. Insbesondere gilt $a\mathbb{Z} \subseteq H$. Die Menge $\{\frac{1}{n} \mid n \in \mathbb{N}\}$ erzeugt die additive Gruppe $\mathbb{Q}$ und da H echt in G enthalten ist, finden wir eine Zahl $n \in \mathbb{N}$ mit $\frac{1}{n} \notin H$. Wir definieren $K = \langle H \cup \{\frac{1}{n}\}\rangle = H + \mathbb{Z}\frac{1}{n}$. Nach Konstruktion gilt $H \subsetneq K$.

Um zu sehen, dass K eine echte Untergruppe ist, zeigen wir, dass das Element $\frac{1}{an^2}$ nicht in K liegt. Dies sieht man durch ein Widerspruchsargument. Angenommen

$\frac{1}{an^2} \in K$, dann gilt

$$h + \frac{c}{n} = \frac{1}{an^2}$$

für $h \in H$ und eine ganze Zahl c. Multiplizieren wir nun mit an, erhalten wir

$$anh + ac = \frac{1}{n}.$$

Wegen $a\mathbb{Z} \subseteq H$, liegt die linke Seite in H. Dies führt zum Widerspruch, denn $\frac{1}{n}$ liegt nicht in H.

II. Primitive Wirkungen

Wir wollen uns nun mit *primitiven* Gruppenwirkungen befassen und werden schließlich feststellen, dass diese eng verwandt sind mit maximalen Untergruppen.

2.2.9 Ist X eine G-Menge, dann definieren wir für jede Teilmenge $B \subseteq X$ und jedes Element $g \in G$

$$g \cdot B = \{g \cdot b \mid b \in B\}.$$

Dies definiert eine Wirkung von G auf der Menge der Teilmengen von X.

2.2.10 **Blöcke**. Es sei G eine Gruppe. Eine Teilmenge $B \subseteq X$ einer G-Menge X heißt *Block*, falls für jedes Element $g \in G$

$$g \cdot B = B \quad \text{oder} \quad B \cap g \cdot B = \emptyset$$

gilt. Natürlich sind X, die leere Menge $\emptyset$ und alle ein-elementigen Mengen $\{x\}$ stets Blöcke. Diese sind aber nicht sehr interessant, deshalb nennen wir diese Blöcke *trivial*.

2.2.11 **Definition**. Eine Wirkung von G auf X heißt *imprimitiv*, wenn es einen nichttrivialen Block $B \subseteq X$ gibt. Andernfalls nennen wir die Wirkung *primitiv*.

2.2.12 Es sei X eine G-Menge. Jede Bahn $B := G \cdot x$ ist ein Block, denn es gilt $g \cdot B = B$ für alle $g \in G$. Interessiert man sich für primitive Wirkungen, dann ist es sinnvoll die Untersuchung auf transitive Wirkungen zu beschränken.

2.2.13 Beispiel. Das typische Beispiel für eine primitive Wirkung ist die Permutationswirkung von S_n auf $\{1, 2, \ldots, n\}$. In der Tat, es sei $B \subsetneq \{1, 2, \ldots, n\}$ eine echte Teilmenge mit $|B| \geq 2$. Wir wollen zeigen, dass B kein Block ist. Dazu wählen wir drei verschiedene Zahlen $i, j, k \in \{1, 2, \ldots, n\}$ mit $i, j \in B$ aber $k \notin B$. Dann gilt

$$(i\ \ k) \cdot B = (\{k\} \cup B) \setminus \{i\} \neq B.$$

Zusätzlich gilt $j \in (i\ \ k) \cdot B$, also $B \cap (i\ \ k) \cdot B \neq \emptyset$. Damit ist B also kein Block.

2.2.14 Beispiel. Es sei E die Menge $\{\pm 1\}^3 \subseteq \mathbb{R}^3$, d.h., E ist die Menge der 8 Ecken eines Würfels mit Seitenlänge 2. Die Symmetriegruppe des Würfels (vgl. 1.2.4)

$$\operatorname{Isom}(\mathbb{R}^3, E) = \{f \in \operatorname{Isom}(\mathbb{R}^n) \mid f(E) = E\}$$

wirkt auf der Menge E der Ecken; siehe 2.1.6. Jede Isometrie bildet ein Paar diagonal gegenüberliegender Ecken wieder auf ein solches Paar ab. In der Tat, zu jeder Ecke δ gibt es genau eine diagonal gegenüberliegende (nämlich $-\delta$). Diese ist die einzige der 8 Ecken, die dem Abstand $2\sqrt{3}$ von δ besitzt.

Damit bildet die Menge $B = \{\delta, -\delta\}$, die aus zwei diagonal gegenüberliegenden Ecken besteht, einen Block. Die Wirkung der Symmetriegruppe auf den Ecken ist also imprimitiv.

2.2.15 Hilfssatz. *Es sei X eine G-Menge und $B \subseteq X$ sei ein Block.*

(i) Für $g, h \in G$ sind die Mengen $g \cdot B$ und $h \cdot B$ entweder gleich oder disjunkt.

(ii) Für jedes Element $b \in B$ gilt $\mathrm{St}_G(b) \subseteq \mathrm{St}_G(B)$

(iii) Ist $B \neq \emptyset$ und die Wirkung von G auf X transitiv, dann ist X die disjunkte Vereinigung

$$X = \bigsqcup_{g \in R} g \cdot B$$

wobei R ein Repräsentantensystem für die Nebenklassen von $\mathrm{St}_G(B)$ ist.

Beweis. (i): Falls $g \cdot B \cap h \cdot B \neq \emptyset$, dann ist $h^{-1}g \cdot B \cap B \neq \emptyset$. Da B ein Block ist, gilt $h^{-1}g \cdot B = B$ und damit auch $g \cdot B = h \cdot B$.

(ii): Es sei $g \in \mathrm{St}_G(b)$ beliebig. Weil nun $b \in g \cdot B \cap B$ gilt, folgt $g \cdot B = B$ und somit $g \in \mathrm{St}_G(B)$.

(iii): Nehmen wir an, dass die Wirkung von G transitiv und B nicht leer ist. Dann ist $X = \bigcup_{g \in G} g \cdot B$. Da die verschobenen Blöcke entweder gleich oder disjunkt sind, müssen wir nur die Vielfachen aussortieren. Es gilt aber $g \cdot B = h \cdot B$ genau dann, wenn $h^{-1}g \in \mathrm{St}_G(B)$ gilt. Also genügt es aus jeder Nebenklasse von $\mathrm{St}_G(B)$ genau einen Vertreter zu wählen. □

2.2.16 Korollar. *Es seien G eine Gruppe und X eine transitive G-Menge. Ist $|X| = p$ eine Primzahl, dann ist die Wirkung primitiv.*

Beweis. Es sei $B \subseteq X$ ein nicht-leerer Block. Nach 2.2.15 (iii) gilt $|X| = |R| \cdot |B|$ und da $|X|$ eine Primzahl ist, muss $|B| = 1$ oder $B = X$ gelten. Der Block ist also trivial und die Wirkung somit primitiv. □

2.2.17 Satz. *Es sei G eine Gruppe, die auf einer Menge X mit $|X| > 1$ transitiv wirkt. Es sei $x \in X$ beliebig. Die Wirkung von G auf X ist genau dann primitiv, wenn der Stabilisator von $\mathrm{St}_G(x)$ eine maximale Untergruppe von G ist.*

Beweis. Wir nehmen zunächst an, dass die Wirkung imprimitiv ist. Es gibt also einen nicht-trivialen Block $B \subseteq X$. Da auch die Mengen $g \cdot B$ Blöcke sind und die Wirkung transitiv ist, können wir $x \in B$ annehmen (das sieht man mit 2.2.15 (iii)).

Wir behaupten, dass $\mathrm{St}_G(x) \subsetneq \mathrm{St}_G(B) \subsetneq G$ gilt. In der Tat, wegen $B \neq X$ und der Transitivität der Wirkung finden wir ein Element $g \in G$ mit $g \cdot x \notin B$; es folgt $\mathrm{St}_G(B) \subsetneq G$. Weil $B \neq \{x\}$ ist und die Wirkung transitiv ist, finden wir ein Element $g' \in G$ mit $g' \cdot x \neq x$ aber $g' \cdot x \in B$. Aus 2.2.15 (i) folgt dann aber $g' \cdot B = B$ und somit $\mathrm{St}_G(x) \subsetneq \mathrm{St}_G(B)$. Also ist $\mathrm{St}_G(x)$ keine maximale Untergruppe.

Umgekehrt sei nun die Wirkung primitiv. Wir zeigen, dass $\mathrm{St}_G(x)$ eine maximale Untergruppe ist. Wir stellen zunächst fest, dass $\mathrm{St}_G(x)$ eine echte Untergruppe ist, denn aus dem Bahn-Stabilisator-Satz 2.1.19 folgt $|G : \mathrm{St}_G(x)| = |X| > 1$.

Sei nun $K \leq G$ mit $\mathrm{St}_G(x) \subsetneq K$. Wir zeigen zunächst, dass $B = K \cdot x$ ein Block ist. Dazu sei $g \in G$. Angenommen es sei $g \cdot B \cap B \neq \emptyset$. Es existieren also $k_1, k_2 \in K$ mit $gk_1 \cdot x = k_2 \cdot x$. Dann ist $k_2^{-1} g k_1 \in \mathrm{St}_G(x) \subsetneq K$ und damit auch $g \in K$, d.h., $g \cdot B = B$.

Weil K echt größer als der Stabilisator $\mathrm{St}_G(x)$ ist, gilt $K \cdot x \supsetneq \{x\}$. Die Wirkung ist aber primitiv und der Block B ist somit trivial, d.h., es muss $B = X$ sein. Für alle $g \in G$ finden wir also ein $k \in K$ dergestalt, dass

$$g \cdot x = k \cdot x$$

gilt. Dann ist aber $g \in k\,\mathrm{St}_G(x) \subseteq K$. Weil $g \in G$ beliebig war, folgt $G = K$. □

III. k-transitive Wirkungen

Es ist im Allgemeinen schwierig zu prüfen, ob eine Wirkung primitiv ist. Deshalb diskutieren wir in diesem Abschnitt die mehrfach transitiven Wirkungen und zeigen, dass diese Wirkungen immer primitiv sind. Das liefert einen guten Weg um die Primitivität einer Wirkung nachzuweisen.

2.2.18 Mehrfache Transitivität. Es sei X eine G-Menge. Für jedes $k \in \mathbb{N}$ erhalten wir eine Wirkung von G auf der Menge der k-Tupel X^k durch

$$g \cdot (x_1, x_2, \ldots, x_k) \coloneqq (g \cdot x_1, g \cdot x_2, \ldots, g \cdot x_k).$$

Dabei ist die Menge

$$X^{[k]} = \{(x_1, x_2, \ldots, x_k) \in X^k \mid x_i \neq x_j \text{ für alle } i \neq j\}$$

der Tupel, die aus paarweise verschiedenen Einträgen bestehen, stabil unter der Wirkung. Das heißt, die G-Wirkung schränkt sich zu einer Wirkung auf $X^{[k]}$ ein.

Die Wirkung von G auf X heißt *k-transitiv*, wenn $|X| \geq k$ gilt und die Wirkung von G auf $X^{[k]}$ transitiv ist.

Die 1-transitiven Wirkungen sind genau die transitiven. Eine k-transitive Wirkung ist natürlich auch $(k-1)$-transitiv, denn die Projektion $X^{[k]} \to X^{[k-1]}$ auf die ersten $(k-1)$-Einträge ist äquivariant.

2.2.19 Beispiel. Die Wirkung der symmetrischen Gruppe S_n auf $\{1,2,\ldots,n\}$ ist n-transitiv. In der Tat, sind $(k_1,k_2,\ldots,k_n)$ und $(k'_1,\ldots,k'_n)$ zwei n-Tupel in $\{1,2,\ldots,n\}^{[n]}$, dann kommt jede Zahl aus $\{1,2,\ldots,n\}$ genau einmal in jedem Tupel vor. Also definiert $\sigma(k_i) := k'_i$ eine Permutation in S_n die

$$\sigma \cdot (k_1,k_2,\ldots,k_n) = (k'_1,\ldots,k'_n)$$

erfüllt.

2.2.20 Aufgabe. Zeigen Sie: die Wirkung der symmetrischen Gruppe $\mathrm{Sym}(\mathbb{N})$ auf $\mathbb{N}$ ist k-transitiv für jedes $k \in \mathbb{N}$. L

2.2.21 Beobachtung. Es seien G eine Gruppe und X eine G-Menge. Für jedes $x \in X$ ist die Menge $X \setminus \{x\}$ eine $\mathrm{St}_G(x)$-Menge bezüglich der eingeschränkten Wirkung. Das sieht man so: Sind $y \in X \setminus \{x\}$ und $g \in \mathrm{St}_G(x)$ gegeben, so gilt auch $g^{-1} \in \mathrm{St}_G(x)$. Angenommen $g \cdot y = x$, dann erhält man durch Wirkung mit g^{-1} die Gleichung $y = g^{-1} \cdot x = x$ und damit einen Wiederspruch. Also gilt $g \cdot y \in X \setminus \{x\}$.

2.2.22 Satz (Kriterium für k-Transitivität). *Es seien X eine transitive G-Menge und $k \geq 2$. Die Wirkung von G auf X ist genau dann k-transitiv, wenn $X \setminus \{x\}$ für alle $x \in X$ eine $(k-1)$-transitive $\mathrm{St}_G(x)$-Menge ist.*

Beweis. Wir bemerken kurz, dass $|X| \geq k$ genau dann gilt, wenn $|X \setminus \{x\}| \geq k-1$ gilt. Angenommen die Wirkung von G auf X ist k-transitiv. Es sei $x \in X$ beliebig; wir definieren $X' = X \setminus \{x\}$. Sind

$$(x_1,\ldots,x_{k-1}),(y_1,\ldots,y_{k-1}) \in X'^{[k-1]}$$

zwei $(k-1)$-Tupel verschiedener Elemente in X', dann sind $(x_1,\ldots,x_{k-1},x)$ und $(y_1,\ldots,y_{k-1},x)$ zwei k-Tupel in $X^{[k]}$. Es gibt also ein Element $g \in G$ dergestalt, dass $g \cdot x_i = y_i$ für alle $i \in \{1,2,\ldots,k-1\}$ und $g \cdot x = x$ gelten. Wegen $g \cdot x = x$ liegt g im Stabilisator $\mathrm{St}_G(x)$.

Nehmen wir nun an, dass die Wirkungen der Stabilisatoren jeweils $(k-1)$-transitiv sind. Es seien

$$(x_1,\ldots,x_k),(y_1,\ldots,y_k) \in X^{[k]}.$$

Da die Wirkung von G auf X transitiv ist, finden wir ein Element $h \in G$ mit $h \cdot y_1 = x_1$. Wegen $h \cdot (y_1, \ldots, y_k) \in X^{[k]}$ gilt $h \cdot y_i \neq x_1$ für alle $i \geq 2$. Da die Wirkung von $\mathrm{St}_G(x_1)$ auf $X \setminus \{x_1\}$ nach Voraussetzung $(k-1)$-transitiv ist, finden wir ein $g \in \mathrm{St}_G(x_1)$ mit

$$g \cdot (x_2, \ldots, x_k) = (h \cdot y_2, \ldots, h \cdot y_k).$$

Also erfüllt das Element $h^{-1}g$ die Bedingung

$$h^{-1}g \cdot (x_1, \ldots, x_k) = h^{-1} \cdot (x_1, h \cdot y_2 \ldots, h \cdot y_k) = (y_1, y_2 \ldots, y_k). \qquad \square$$

2.2.23 **Satz.** *Jede 2-transitive Wirkung ist primitiv.*

Beweis. Es sei X eine 2-transitive G-Menge. Wir wollen zeigen, dass jeder Block trivial ist. Dazu nehmen wir eine echte Teilmenge $B \subsetneq X$ mit $|B| \geq 2$ und zeigen, dass B kein Block ist.

Wir finden verschiedene Elemente $x, y, z \in X$ mit $x, y \in B$ aber $z \notin B$. Weil die Wirkung 2-transitiv ist, gibt es $g \in G$ dergestalt, dass $g \cdot (x, y) = (x, z)$ gilt. Daraus folgt $g \cdot B \neq B$, denn $z \in g \cdot B$. Zusätzlich ist $x \in g \cdot B \cap B$, also ist B kein Block. $\square$

2.2.24 **Aufgabe.** Zeigen Sie, dass die Wirkung der alternierenden Gruppe A_n auf $\{1, 2, \ldots, n\}$ 2-transitiv ist, falls $n \geq 4$ gilt. **L**

2.3. Direkte Produkte

2.3.1 In diesem Abschnitt werden wir ein einfaches Verfahren kennenlernen, mit dem man viele neue Beispiele von Gruppen konstruieren kann: das direkte Produkt.

2.3.2 **Das direkte Produkt zweier Gruppen**. Es seien G_1, G_2 zwei Gruppen. Auf dem kartesischen Produkt

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$$

definieren wird eine Gruppenstruktur, indem wir das Produkt von Paaren komponentenweise definieren, d.h.,

$$(g_1, g_2)(h_1, h_2) := (g_1 h_1, g_2 h_2).$$

für alle $g_1, h_1 \in G_1$ und $g_2, h_2 \in G_2$. Dabei ist natürlich in der ersten Komponente die Gruppenmultiplikation aus G_1 und in der zweiten Komponente die Gruppenmultiplikation aus G_2 gemeint. Das Assoziativgesetz für die neue Multiplikation lässt sich direkt aus Assoziativität der beiden Gruppenmultiplikationen herleiten. Für alle $g_1, h_1, k_1 \in G_1$ und $g_2, h_2, k_2 \in G_2$ gilt

$$\begin{aligned} \big((g_1, g_2)(h_1, h_2)\big)(k_1, k_2) =& (g_1 h_1, g_2 h_2)(k_1, k_2) = ((g_1 h_1)k_1, (g_2 h_2)k_2) \\ =& (g_1(h_1 k_1), g_2(h_2 k_2)) = (g_1, g_2)\big((h_1, h_2)(k_1, k_2)\big). \end{aligned}$$

Das Paar (e_{G_1}, e_{G_2}) ist ein neutrales Element für die Multiplikation, denn

$$(e_{G_1}, e_{G_2})(g_1, g_2) = (e_{G_1} g_1, e_{G_2} g_2) = (g_1, g_2) = (g_1, g_2)(e_{G_1}, e_{G_2}).$$

Offensichtlich ist das Element (g_1^{-1}, g_2^{-1}) invers zu (g_1, g_2) und damit ist $G_1 \times G_2$ eine Gruppe. Die Gruppe $G_1 \times G_2$ nennt man das *direkte Produkt* der Gruppen G_1 und G_2.

2.3.3 **Direkte Produkte allgemein**. Die Konstruktion und der Beweis in 2.3.2 verwenden nirgends die Tatsache, dass wir das kartesische Produkt von *zwei* Gruppen gebildet haben. Genauso kann man das direkte Produkt von drei, vier, fünf oder unendlich vielen Gruppen konstruieren. Es sei also $(G_i)_{i \in I}$ eine Familie von Gruppen, die durch eine beliebige Indexmenge I parametrisiert wird. Zum

Beispiel kann man $I = \{1,2\}$, $I = \{1,2,3\}$ oder $I = \mathbb{N}$ wählen. Erweitert man den Beweis aus 2.3.2 von zwei auf beliebig viele Faktoren (Übungsaufgabe!), **L**
dann erhält man folgenden Satz:

Das kartesische Produkt

$$\prod_{i \in I} G_i = \{(g_i)_{i\in I} \mid g_i \in G_i\}$$

bildet zusammen mit der Multiplikation

$$(g_i)_{i\in I}(h_i)_{i\in I} \coloneqq (g_i h_i)_{i\in I}$$

eine Gruppe. Das neutrale Element ist $(e_{G_i})_{i\in I}$ *und das inverse Element zu* $(g_i)_{i\in I}$ *ist* $(g_i^{-1})_{i\in I}$.

Die Gruppe $\prod_{i\in I} G_i$ nennt man das *direkte Produkt* der Gruppen $(G_i)_{i\in I}$.

2.3.4 **Projektionen**. Wir betrachten das direkte Produkt $\prod_{i\in I} G_i$. Es sei $j \in I$.

Die Projektion $\pi_j \colon \prod_{i\in I} G_i \to G_j$ *auf die* j*-te Komponente – also die Abbildung* $(g_i)_{i\in I} \mapsto g_j$ *– ist ein surjektiver Gruppenhomomorphismus.*

Sicherlich ist π_j surjektiv. Die folgende Rechnung zeigt, dass π_j ein Homomorphismus ist:

$$\pi_j\big((g_i)_{i\in I}(h_i)_{i\in I}\big) = \pi_j\big((g_i h_i)_{i\in I}\big) = g_j h_j = \pi_j\big((g_i)_{i\in I}\big)\pi_j\big((h_i)_{i\in I}\big).$$

Es ist sehr nützlich Konstruktionen wie das direkte Produkt anhand ihrer *universellen Eigenschaften* zu untersuchen. Das wird in der Kategorientheorie systematisch versucht. Das direkte Produkt von Gruppen, das wir gerade konstruiert haben, besitzt also die universelle Eigenschaft des direkten Produktes im Sinne der Kategorientheorie.

2.3.5 **Universelle Eigenschaft des direkten Produktes**. *Es seien* H *eine Gruppe und* $(G_i)_{i\in I}$ *eine Familie von Gruppen. Ist für jedes* $i \in I$ *ein Homomorphismus* $\alpha_i \colon H \to G_i$ *gegeben, dann existiert ein eindeutiger Homomorphismus* $\Pi\alpha \colon H \to \prod_{i\in I} G_i$*, sodass*

$$\pi_j \circ \Pi\alpha = \alpha_j$$

für alle $j \in I$. Das folgende Diagramm ist also kommutativ für alle $j \in I$:

$$\begin{tikzcd} H \arrow[rr, dashed, "\Pi\alpha"] \arrow[dr, "\alpha_j"'] & & \prod_{i\in I} G_i \arrow[dl, "\pi_j"] \\ & G_j & \end{tikzcd}$$

Beweis. Wir definieren $\Pi\alpha(h) \coloneqq (\alpha_i(h))_{i\in I}$, denn dann (und nur dann!) gilt die gewünschte Eigenschaft

$$\pi_j(\Pi\alpha(h)) = \alpha_j(h).$$

Man muss nur prüfen, dass $\Pi\alpha$ ein Homomorphismus ist, aber das ist eine leichte Übungsaufgabe. □ **L**

Wir wollen nun ein Kriterium herleiten, mit dem man feststellen kann, ob eine Gruppe das direkte Produkt zweier Normalteiler ist. Dazu benötigen wir folgende Beobachtung.

2.3.6 Hilfssatz. *Es seien G eine Gruppe und $N, M \trianglelefteq G$ zwei Normalteiler. Dann gilt*

$$[N, M] \subseteq N \cap M.$$

Falls $N \cap M = \{e\}$ ist, dann kommutieren die Elemente von N und M paarweise.

Beweis. Es seien $n \in N$ und $m \in M$. Dann gilt

$$[n, m] = nmn^{-1}m^{-1} = n\underbrace{(mn^{-1}m^{-1})}_{\in N} = \underbrace{(nmn^{-1})}_{\in M}m^{-1} \in N \cap M.$$

Ist der Schnitt $N \cap M$ trivial, dann folgt $[N, M] = \{e\}$ und die Elemente von N und M vertauschen; siehe 1.4.11. □

2.3.7 Satz. *Es sei G eine Gruppe. Sind N, M Normalteiler von G mit $N \cap M = \{e\}$, dann ist die Abbildung*

$$p\colon N \times M \to G \quad \text{mit} \quad (n, m) \mapsto nm$$

ein injektiver Homomorphismus von Gruppen. Gilt zusätzlich $NM = G$, dann ist p ein Isomorphismus.

Beweis. Aus 2.3.6 folgt, dass die Elemente von N und M paarweise vertauschen. Damit ist p ein Homomorphismus, denn

$$p((n,m)(n',m')) = p(nn',mm') = nn'mm' = nmn'm' = p(n,m)p(n',m')$$

für alle $n, n' \in N$ und $m, m' \in M$. Es sei $(n,m) \in \mathrm{Ker}(p)$, dann gilt $nm = e$ und somit $n = m^{-1} \in N \cap M$. Weil der Schnitt $N \cap M$ trivial ist folgt $(n,m) = (e,e)$ und damit ist p injektiv.

Gilt auch $NM = G$, dann ist p auch surjektiv und damit ein Isomorphismus. □

2.3.8 **Aufgabe**. Unter geeigneten Voraussetzungen lassen sich die Aussage und der Beweis von 2.3.7 von zwei auf endlich viele Normalteiler verallgemeinern. **L**

Formulieren Sie passende Bedingungen für drei Normalteiler und nutzen Sie diese um 2.3.7 zu verallgemeinern.

2.3.9 **Korollar**. *Es seien m_1, m_2 teilerfremde natürliche Zahlen und $n = m_1 m_2$. Dann gibt es einen Isomorphismus*

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}.$$

Beweis. Nach dem Satz über die zyklischen Gruppen 1.5.1 hat $\mathbb{Z}/n\mathbb{Z}$ zwei zyklische Untergruppen M_1 und M_2 der Ordnung m_1 bzw. m_2. Weil m_1 und m_2 teilerfremd sind, folgt aus dem Satz von Lagrange 1.2.21 bereits

$$M_1 \cap M_2 = \{e\}.$$

Aus 2.3.7 erhalten wir einen injektiven Homorphismus $p\colon M_1 \times M_2 \to \mathbb{Z}/n\mathbb{Z}$. Da beide Gruppen die Ordnung $n = m_1 m_2$ haben, ist p auch surjektiv und damit ein Isomorphismus. □

Durch wiederholte Anwendung von 2.3.9 erhalten wir:

2.3.10 Korollar. *Es sei $m \in \mathbb{N}$ mit Primfaktorzerlegung*[5] $m = p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k}$. *Dann gilt*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{f_1}\mathbb{Z} \times \mathbb{Z}/p_2^{f_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{f_k}\mathbb{Z}.$$

2.3.11 Das beschränkte direkte Produkt. Es sei I eine (unendliche) Indexmenge und $(G_i)_{i\in I}$ eine Familie von Gruppen. Die Elemente $(g_i)_{i\in I}$ mit $g_i = e_{G_i}$ für fast alle i – d.h., für alle bis auf endlich viele $i \in I$ – bilden eine Untergruppe des direkten Produktes $\prod_{i\in I} G_i$. Wir nennen diese Untergruppe das *beschränkte direkte Produkt* und bezeichnen sie mit

$$\prod_{i\in I}{}' G_i = \Big\{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid g_i = e_{G_i} \text{ für fast alle } i \in I\Big\}.$$

Für endliche Indexmengen gibt es natürlich keinen Unterschied zwischen dem direkten Produkt und dem beschränkten direkten Produkt. Das beschränkte direkte Produkt wird von den Elementen erzeugt, die genau einen Eintrag $g_i \neq e$ besitzen.

2.3.12 Vorsicht. Für das beschränkte direkte Produkt kursieren diverse Namen in der Literatur, z.B., „direkte Summe“. Andere Autoren bezeichnen unser direktes Produkt als „unbeschränktes direktes Produkt“ und verwenden die Bezeichnung direktes Produkt im beschränkten Fall.

2.3.13 Bemerkung. Das beschränkte direkte Produkt über einer unendliche Indexmenge ist gewissermaßen „deutlich kleiner“ als das direkte Produkt. Zum Beispiel ist das beschränkte direkte Produkt

$$\prod_{i\in\mathbb{N}_0}{}' \mathbb{Z}/2\mathbb{Z}$$

abzählbar unendlich. Um das zu sehen, kann man die Elemente mittels des Binärsystems den natürlichen Zahlen zuordnen. Andererseits folgt aus dem Cantor'schen[6] Diagonalargument, dass das direkte Produkt $\prod_{i\in\mathbb{N}_0} \mathbb{Z}/2\mathbb{Z}$ überabzählbar ist.

2.3.14 Inklusionsabbildungen. Es sei I eine Indexmenge und $(G_i)_{i\in I}$ eine Familie

[5]Die Primzahlen $p_1, \dots, p_k$ sind also paarweise verschieden.
[6]Georg Cantor: deutscher Mathematiker, 1845 – 1918.

von Gruppen. Für jedes $j \in I$ ist die „Inklusionsabbildung“ $\iota_j\colon G_j \to \prod'_{i\in I} G_i$ ein Homomorphismus. Diese Abbildung bildet $g \in G_j$ auf $(g_i)_{i\in I}$ ab, wobei $g_j = g$ und $g_i = e$ für alle $i \neq j$ ist.

2.3.15 Universelle Eigenschaft des beschränkten direkten Produktes. *Das beschränkte direkte Produkt $\prod'_{i\in I} G_i$ einer Familie $(G_i)_{i\in I}$ von Gruppen erfüllt folgende universelle Eigenschaft:*

Es seien G eine Gruppe und $\alpha_i\colon G_i \to G$ eine Familie von Homomorphismen. Falls für alle $i \neq j$ die Bilder von α_i und α_j elementweise vertauschen, dann existiert ein eindeutiger Homomorphismus

$$\prod_{i\in I}{}' \alpha_i\colon \prod_{i\in I}{}' G_i \to G,$$

mit $(\prod'_{i\in I} \alpha_i) \circ \iota_j = \alpha_j$ für alle $j \in I$.

$$\begin{tikzcd} G_j \arrow[r, "\iota_j"] \arrow[dr, "\alpha_j"'] & \prod'_{i\in I} G_i \arrow[d, dashed, "\prod'_{i\in I} \alpha_i"] \\ & G \end{tikzcd}$$

Beweis. Es seien G eine Gruppe und $\alpha_i\colon G_i \to G$ eine Familie von Homomorphismen. Wir zeigen zuerst die Existenz des Homomorphismus $\prod'_{i\in I} \alpha_i$. Es sei $g = (g_i)_{i\in I} \in \prod'_{i\in I} G_i$. Nach Definition des beschränkten direkten Produktes ist die Teilmenge $S(g) = \{i \in I \mid g_i \neq e\}$ endlich. Ordnen wir die Elemente von $S(g)$ beliebig an, sagen wir $S(g) = \{i_1, i_2, \ldots, i_k\}$, dann ist

$$\beta(g) \coloneqq \alpha_{i_1}(g_{i_1}) \cdot \alpha_{i_2}(g_{i_2}) \cdots \alpha_{i_k}(g_{i_k})$$

ein Element in G. Da die Bilder der Homomorphismen $\alpha_{i_1}, \ldots, \alpha_{i_k}$ paarweise vertauschen, ist die gewählte Reihenfolge dabei unwichtig; wir schreiben daher kurz

$$\beta(g) = \prod_{i\in S(g)} \alpha_i(g_i).$$

Nun prüft man nach, dass β ein Homomorphismus ist (Übungsaufgabe!). Dies ist der gesuchte Homomorphismus, denn wegen $S(\iota_j(g_j)) = \{j\}$ gilt **L**

$$\beta(\iota_j(g_j)) = \alpha_j(g_j)$$

Nun zur Eindeutigkeit: Die Bilder der Inklusionsabbildungen erzeugen das beschränkte Produkt ${\prod}'_{i\in I} G_i$, denn es gilt

$$g = (g_i)_{i\in I} = \prod_{i\in S(g)} \iota_i(g_i).$$

Daraus folgt die Eindeutigkeit (siehe 1.4.8 (ii)). □

2.3.16 Aufgabe. Es sei $(G_i)_{i\in I}$ eine Familie von Gruppen. Zeigen Sie, dass das beschränkte direkte Produkt ${\prod}'_{i\in I} G_i$ ein Normalteiler des direkten Produktes $\prod_{i\in I} G_i$ ist. **L**

2.4. Semidirekte Produkte

2.4.1 Aus Satz 2.3.7 wissen wir, dass eine Gruppe G, die Normalteiler $N, M \trianglelefteq G$ besitzt mit $N \cap M = \{e\}$ und $NM = G$, zum direkten Produkt $N \times M$ isomorph ist. In diesem Fall vertauschen die Elemente von N mit denen von M.

Was passiert aber wenn nur eine der beiden Untergruppen N und M ein Normalteiler ist? Wir wollen hier eine weitere Konstruktion von Gruppen kennenlernen, die das direkte Produkt zweier Faktoren entsprechend verallgemeinert.

I. Konstruktion und Beispiele

2.4.2 **Wirkungen durch Automorphismen**. Es seien H und K zwei Gruppen und

$$H \times N \to N \quad \text{mit} \quad (h, n) \mapsto {}^h n$$

sei eine Gruppenwirkung. Man nennt diese Wirkung eine *Wirkung durch Automorphismen*, wenn für jedes $h \in H$ die Abbildung $\lambda_h \colon n \mapsto {}^h n$ ein Automorphismus von N ist.

2.4.3 **Anmerkungen zur Definition**.

(a) Die Notation ${}^h n$ erinnert an die Konjugation und wir werden bald sehen, warum das sinnvoll ist.

(b) Da die Abbildung $\lambda_h \colon n \mapsto {}^h n$ stets bijektiv ist (siehe 2.1.3 (b)), handelt es sich genau dann um eine Wirkung durch Automorphismen, wenn jedes λ_h ein Homomorphismus ist, d.h., wenn

$${}^h(nm) = {}^h n {}^h m$$

für alle $h \in H$ und $n, m \in N$ gilt.

(c) In 2.1.3 (c) haben wir gesehen, dass die Abbildung $\lambda \colon H \to \mathrm{Sym}(N)$ mit $h \mapsto \lambda_h$ ein Homomorphismus von Gruppen ist. Die Wirkung ist genau dann eine Wirkung durch Automorphismen, wenn das Bild von λ in der Automorphismengruppe $\mathrm{Aut}(N)$ liegt.

2.4.4 **Beispiel**. Es seien G eine Gruppe und N, H Untergruppen. Falls $H \subseteq N_G(N)$ im Normalisator von N liegt, dann gilt

$$^h n = hnh^{-1} \in N$$

für alle $n \in N$ und $h \in H$. Die Konjugationswirkung $H \times N \to N$ mit $(h, n) \mapsto {}^h n$ ist dann eine Wirkung von H auf N durch Automorphismen, denn

$$^h(nm) = hnmh^{-1} = hnh^{-1}hmh^{-1} = {}^h n {}^h m.$$

2.4.5 **Beispiel**. Es sei G eine Gruppe. Die Automorphismengruppe $\mathrm{Aut}(G)$ wirkt auf G durch Automorphismen vermöge

$$\mathrm{Aut}(G) \times G \to G \quad \text{mit} \quad (\alpha, g) \mapsto \alpha(g).$$

Es handelt sich dabei um die Einschränkung der Wirkung von $\mathrm{Sym}(G)$ auf G (siehe Beispiel 2.1.4) auf die Untergruppe $\mathrm{Aut}(G)$.

2.4.6 **Das semidirekte Produkt**. Es seien H und N Gruppen und es sei

$$w \colon H \times N \to N \quad \text{mit} \quad w(h, n) = {}^h n$$

eine Wirkung durch Automorphismen. Wir betrachten die Menge $N \times H$ und definieren darauf die Verknüpfung

$$(n, h) *_w (m, k) := (n {}^h m, hk).$$

Wir wollen zeigen, dass diese Verknüpfung eine Gruppenstruktur auf $N \times H$ definiert. Dazu prüfen wir zunächst die Assoziativität. Es seien dazu $h_1, h_2, h_3 \in H$ und $n_1, n_2, n_3 \in N$.

$$\begin{aligned}
\big((n_1, h_1) *_w (n_2, h_2)\big) *_w (n_3, h_3) &= (n_1 {}^{h_1} n_2, h_1 h_2) *_w (n_3, h_3) \\
&= (n_1 {}^{h_1} n_2 {}^{h_1 h_2} n_3, h_1 h_2 h_3) = (n_1 {}^{h_1}(n_2 {}^{h_2} n_3), h_1 h_2 h_3) \\
&= (n_1, h_1) *_w (n_2 {}^{h_2} n_3, h_2 h_3) = (n_1, h_1) *_w \big((n_2, h_2) *_w (n_3, h_3)\big)
\end{aligned}$$

Das Element (e_N, e_H) ist das links-neutrale Element, denn es gilt

$$(e_N, e_H)(n, h) = (e_N{}^{e_H}n, e_H h) = ({}^{e_H}n, h) = (n, h);$$

dabei folgt der letzte Schritt aus dem Gruppenwirkungsaxiom (W1). Das Links-inverse von (n, h) ist $({}^{h^{-1}}n^{-1}, h^{-1})$, denn wir erhalten

$$({}^{h^{-1}}n^{-1}, h^{-1}) *_w (n, h) = ({}^{h^{-1}}n^{-1}{}^{h^{-1}}n, h^{-1}h) = ({}^{h^{-1}}(n^{-1}n), e_H) = (e_N, e_H).$$

Die Gruppe $(N \times H, *_w)$ heißt das *semidirekte Produkt* der von N mit H bezüglich der Wirkung w. Wir verwenden die Notation $N \rtimes_w H$ für das semidirekte Produkt bezüglich w. Falls die Wirkung w aus dem Kontext klar hervorgeht, lässt man den Index w meistens weg. Wie in jeder Gruppe verschweigen wir beim Rechnen meistens das Symbol $*_w$ für die Gruppenmultiplikation.

2.4.7 **Satz**. *Das semidirekte Produkt $N \rtimes_w H$ ist eine Gruppe mit der Multiplikation*

$$(n, h) *_w (m, k) = (n{}^h m, hk).$$

Das neutrale Element ist (e_N, e_H) und das Inverse zu (n, h) ist $({}^{h^{-1}}n^{-1}, h^{-1})$. Die Abbildungen $i_N \colon N \to N \rtimes_w H$ mit $i_N(n) = (n, e_H)$ und $i_H \colon H \to N \rtimes_w H$ mit $i_H(h) = (e_N, h)$ sind injektive Homomorphismen. Das Bild von i_N

$$i_N(N) := \big\{(n, e_H) \in N \rtimes_w H\big\}$$

ist ein Normalteiler von $N \rtimes_w H$. Die Konjugationswirkung von $i_H(H)$ auf $i_N(N)$ ist durch

$$(e_N, h)(n, e_H)(e_N, h^{-1}) = ({}^h n, e_H).$$

gegeben.

Beweis. Den ersten Teil haben wir schon in 2.4.6 bewiesen. Wir müssen nun noch die Aussagen über i_N und i_H beweisen. Zunächst stellen wir fest, dass

$$(n, e)(m, e) = (nm, e) \quad \text{und} \quad (e, h)(e, k) = (e, hk)$$

gelten. Aus dieser Rechnung folgt direkt, dass die Abbildungen i_N und i_H

Gruppenhomomorphismen sind. Da der Kern jeweils trivial ist, sind diese injektiv; siehe 1.2.10. Für alle $n, m \in N$ und $h \in H$ gilt

$$(m,h)(n,e)({}^{h^{-1}}m^{-1}, h^{-1}) = (m\,{}^{h}n, h)({}^{h^{-1}}m^{-1}, h^{-1}) = (m\,{}^{h}n m^{-1}, e) \in i_N(N),$$

also ist $i_N(N)$ ein Normalteiler. Die Aussage über die Konjugationswirkung erhält man, indem man $m = e$ setzt. □

2.4.8 **Beispiel** (Diedergruppen). Wir betrachten die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ der Ordnung $n \geq 2$. Die zweielementige Gruppe $\{\pm 1\}$ wirkt auf $\mathbb{Z}/n\mathbb{Z}$ durch Multiplikation, d.h.,

$$(\delta, k) \mapsto \delta k.$$

Das Element 1 wirkt also durch die Identität und das Element -1 durch Inversion (siehe 1.1.19); es handelt sich also um eine Wirkung durch Automorphismen. Das semidirekte Produkt

$$D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$$

heißt die *Diedergruppe*[7] der Ordnung $2n$. Das neutrale Element ist also $(\overline{0}, 1)$

Die Diedergruppen sind wichtige Beispiele endlicher Gruppen, deshalb wollen wir uns einige ihrer Eigenschaften anschauen. Wir betrachten nun die Elemente

$$r = (\overline{1}, 1) \quad \text{und} \quad s = (\overline{0}, -1)$$

in der Diedergruppe. Das Element r ist ein Element der Ordnung n und s ist ein Element der Ordnung 2. Es gilt außerdem

$$[r,s] = rsr^{-1}s^{-1} = (\overline{1}, 1)(\overline{0}, -1)(\overline{-1}, 1)(\overline{0}, -1) = (\overline{2}, 1) = r^2.$$

Insbesondere ist die Diedergruppe D_{2n} für $n > 2$ nicht abelsch (denn $r^2 \neq e$). Multiplizieren wir noch von links mit r^{-1} und verwenden $s^{-1} = s$, dann erhalten wir die Relation $srs = r^{-1}$

Die Elemente r und s erzeugen die Diedergruppe D_{2n}. Um das einzusehen

[7] Sprich: Di-Eder

nehmen wir ein beliebiges Element $x = (\overline{k}, \delta) \in D_{2n}$. Falls $\delta = 1$, dann gilt $x = r^k$. Andernfalls ist $\delta = -1$ und es gilt $x = r^k s$.

Das Element $t = rs$ ist ebenfalls ein Element der Ordnung 2, denn

$$t^2 = rsrs = r(srs) = rr^{-1} = e.$$

Natürlich gilt $r = ts$, deshalb kann D_{2n} von den beiden Elementen s, t der Ordnung 2 erzeugt werden.

(Bei der Notation für die Diedergruppe muss man etwas aufpassen. In manchen Texten wird die Bezeichnung D_n anstelle von D_{2n} verwendet.)

2.4.9 Warnung. In der Diedergruppe D_{2n} gilt $\mathrm{ord}(t) = \mathrm{ord}(s) = 2$, aber $\mathrm{ord}(ts) = n$. Insbesondere sehen wir, dass die Ordnung von gh im Allgemeinen nicht mit den Ordnungen von g und h ausgerechnet werden kann.

2.4.10 Beispiel. Man kann die Konstruktion der Diedergruppen etwas verallgemeinern. Es sei $(A, +)$ eine abelsche Gruppe. Die zweielementige Gruppe $\{\pm 1\}$ wirkt auf A, wobei wieder -1 als Inversion wirkt; vgl. 1.1.19. Man erhält dann das semidirekte Produkt $A \rtimes \{\pm 1\}$. Führt man diese Konstruktion mit $A = \mathbb{Z}$ aus, dann erhält man die *unendliche Diedergruppe*

$$D_\infty = \mathbb{Z} \rtimes \{\pm 1\}.$$

2.4.11 Aufgabe. **L**

(a) Zeigen Sie, dass die unendliche Diedergruppe D_∞ von zwei Elementen der Ordnung 2 erzeugt wird.

(b) Zeigen Sie, dass für jedes $n \geq 2$ die Diedergruppe D_{2n} isomorph zu einer Faktorgruppe von D_∞ ist.

2.4.12 Beispiel (Der Holomorph einer Gruppe). Es sei G eine Gruppe. Wir betrachten die natürliche Wirkung von $\mathrm{Aut}(G)$ auf G; siehe 2.4.5. Das semidirekte Produkt $G \rtimes \mathrm{Aut}(G)$ zu dieser Wirkung heißt der *Holomorph* von G. Als Notation verwenden wir

$$\mathrm{Hol}(G) := G \rtimes \mathrm{Aut}(G).$$

Das Produkt zweier Elemente $(g, \alpha), (h, \beta) \in \mathrm{Hol}(G)$ im Holomorph ist also

$$(g, \alpha)(h, \beta) = (g\alpha(h), \alpha \circ \beta).$$

2.4.13 Aufgabe. **L**

(a) Zeigen Sie, dass der Holomorph der unendlichen zyklischen Gruppe $\mathbb{Z}$ isomorph zur unendlichen Diedergruppe D_∞ ist.

(b) Wie viele Elemente hat der Holomorph $\mathrm{Hol}(\mathbb{Z}/m\mathbb{Z})$ einer endlichen zyklischen Gruppe?

II. Universelle Eigenschaft und Anwendungen

Auch das semidirekte Produkt kann mithilfe einer universellen Eigenschaft beschrieben werden.

2.4.14 Universelle Eigenschaft des semidirekten Produktes. *Es seien N und H Gruppen und $w : (h, n) \mapsto {}^h n$ eine Wirkung von H auf N durch Automorphismen. Ist G eine Gruppe und sind $f_H \colon H \to G$ und $f_N \colon N \to G$ Homomorphismen mit der Eigenschaft*

$$f_H(h) f_N(n) f_H(h)^{-1} = f_N({}^h n)$$

für alle $h \in H$ und $n \in N$, dann gibt es einen eindeutigen Homomorphismus $\hat{f} \colon N \rtimes_w H \to G$, sodass $\hat{f} \circ i_N = f_N$ und $\hat{f} \circ i_H = f_H$ gelten.

In anderen Worten, das folgende Diagramm kommutiert

$$\begin{tikzcd}
H \arrow[dr, "i_H"'] \arrow[drr, bend left, "f_H"] & & \\
& N \rtimes_w H \arrow[r, dashed, "\hat{f}"] & G \\
N \arrow[ur, "i_N"] \arrow[urr, bend right, "f_N"'] & &
\end{tikzcd}$$

<u>*Beweis.*</u> Wir überlegen uns zunächst die Eindeutigkeit. Es gilt $i_N(N) i_H(H) = N \rtimes_w H$, daher erzeugt die Menge $i_N(N) \cup i_H(H)$ das semidirekte Produkt. Aus

1.4.8 folgt nun, dass ein Homomorphismus $\hat{f}\colon N \rtimes_w H \to G$ schon eindeutig bestimmt ist, wenn wir wissen was $\hat{f}$ auf den Mengen $i_N(N)$ und $i_H(H)$ macht.

Wir müssen nun noch zeigen, dass $\hat{f}$ existiert. Dazu definieren wir

$$\hat{f}(n,h) = f_N(n)f_H(h).$$

Es gelten nun $\hat{f} \circ i_N = f_N$ und $\hat{f} \circ i_H = f_H$. Die folgende Rechnung zeigt, dass $\hat{f}$ ein Homomorphismus ist:

$$\begin{aligned}\hat{f}((n,h)(m,k)) &= \hat{f}(n^h m, hk) = f_N(n^h m)f_H(hk)\\ &= f_N(n)f_N({}^h m)f_H(h)f_H(k)\\ &= f_N(n)f_H(h)f_N(m)f_H(h)^{-1}f_H(h)f_H(k)\\ &= f_N(n)f_H(h)f_N(m)f_H(k) = \hat{f}(n,h)\hat{f}(m,k).\end{aligned}$$ □

2.4.15 Die Symmetriegruppe des regelmässigen n-Ecks. Es seien $n \geq 3$ und

$$M_n = \{\exp(\frac{2\pi i k}{n}) \in \mathbb{C} \mid k \in \{0, \ldots, n-1\}\}$$

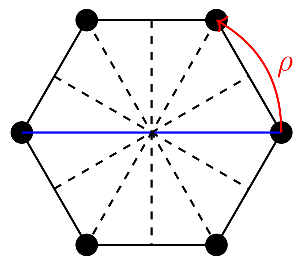
die Menge der Ecken des regelmäßigen n-Ecks mit Mittelpunkt 0 in $\mathbb{C}$. Wir wollen zeigen, dass die Isometriegruppe

$$\mathrm{Isom}(\mathbb{C}, M_n) = \{f \in \mathrm{Isom}(\mathbb{C}) \mid f(M_n) = M_n\}$$

isomorph zur Diedergruppe D_{2n} ist. Eine Isometrie von $\mathbb{C}$ ist hier eine Abbildung, die die übliche Metrik $d(z,w) = |z-w|$ erhält.

Es sei $f \in \mathrm{Isom}(\mathbb{C}, M_n)$. Wir beginnen mit einer Beobachtung: f ist durch die Werte $f(1)$ und $f(\exp(\frac{2\pi i}{n}))$ eindeutig bestimmt, denn jede andere Ecke ist eindeutig durch Ihre Abstände zu 1 und $\exp(\frac{2\pi i}{n})$ festgelegt.

Damit zeigen wir nun, dass $\mathrm{Isom}(\mathbb{C}, M_n)$ höchstens $2n$ Elemente besitzt. In der Tat, es gibt n Ecken, also höchstens n Möglichkeiten für $f(1)$. Da Isometrien Abstände erhalten, muss die von 1 „benachbarte“ Ecke $\exp(\frac{2\pi i}{n})$ auf eine Nachbarecke von $f(1)$ abgebildet werden. Dafür gibt es höchstens 2 Möglichkeiten.



Es ist aber nicht schwierig $2n$ verschieden Isometrien des n-Ecks anzugeben. Wir haben die identische Abbildung, $n-1$ Drehungen

$$\rho, \rho^2, \ldots, \rho^{n-1}$$

(sagen wir gegen den Uhrzeigersinn, d.h., $\rho(z) = \exp(\frac{2\pi i}{n})z$) und n Spiegelungen. Es sei σ die Spieglung an der reellen Achse. Die verschiedenen Spiegelungen sind dann gerade die Elemente

$$\sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma.$$

Weiter gilt $\sigma\rho\sigma = \rho^{-1}$ (wie bereits erwähnt, genügt es diese Gleichheit auf zwei benachbarten Ecken zu prüfen). Die Drehungen bilden eine zyklische Untergruppe der Ordnung n und die Spiegelung σ erzeugt eine zweielementige Untergruppe. Da die Konjugationswirkung von σ auf der Gruppe der Drehungen genau die Inversion ist, liefert uns die universelle Eigenschaft des semidirekten Produktes einen Homomorphismus

$$D_{2n} \to \mathrm{Isom}(\mathbb{C}, M_n)$$

mit $(k+n\mathbb{Z}, 1) \mapsto \rho^k$ und $(k+n\mathbb{Z}, -1) \mapsto \rho^k\sigma$. Da wir alle Elemente von $\mathrm{Isom}(\mathbb{C}, M_n)$ bestimmt haben, sehen wir, dass die Abbildung surjektiv ist. Beide Gruppen haben die Ordnung $2n$, also handelt es sich schon um einen Isomorphismus.

2.4.16 Definition (Komplement). Es seien G eine Gruppe und $K \leq G$ eine Untergruppe. Eine Untergruppe $H \leq G$ heißt *Komplement* von K in G, wenn $K \cap H = \{e\}$ und $KH = G$ gelten.

2.4.17 Satz. *Es sei G eine Gruppe. Sind $N \trianglelefteq G$ ein Normalteiler und $H \leq G$ ein Komplement von N in G, dann gilt*

$$N \rtimes_w H \cong G$$

wobei $w(n,h) = {}^h n$ die Konjugationswirkung von H auf N ist.

2.4.18 Sind die Voraussetzungen des Satzes erfüllt, dann nennt man G das semidirekte Produkt von N und H, wobei man die Konjugationswirkung nicht mehr explizit erwähnt.

Beweis. Es seien $f_H\colon H \to G$ und $f_N\colon N \to G$ die Inklusionsabbildungen. Es gilt $f_H(h)f_N(n)f_H(h)^{-1} = hnh^{-1} = {}^h n$, deshalb liefert uns die universelle Eigenschaft des semidirekten Produktes 2.4.14 einen Homomorphismus von Gruppen

$$\hat{f}\colon N \rtimes_w H \to G \quad \text{mit} \quad \hat{f}(n,h) = nh.$$

Nach Voraussetzung ist $G = NH$ und $\hat{f}$ ist daher surjektiv. Außerdem hat $\hat{f}$ einen trivialen Kern und ist somit injektiv; siehe 1.2.10. In der Tat, es gilt $\hat{f}(n,h) = e$ nur dann, wenn $n = h^{-1} \in N \cap H = \{e\}$ liegt. □

2.4.19 **Beispiel**. Die symmetrische Gruppe S_n (mit $n \geq 2$) ist isomorph zu einem semidirekten Produkt der Form $A_n \rtimes \mathbb{Z}/2\mathbb{Z}$. Dies kann man anhand von Satz 2.4.17 schnell einsehen, denn $A_n \trianglelefteq S_n$ ist ein Normalteiler von Index 2 und die zweielementige Gruppe $\langle(1\ \ 2)\rangle$ ist ein Komplement von A_n in S_n.

2.4.20 **Beispiel** (Die affine Gruppe). Es sei K ein Körper. Eine Abbildung $f_{v,A}\colon K^n \to K^n$ der Form

$$f_{v,A}(x) = v + Ax$$

mit $A \in \mathrm{GL}_n(K)$ und $v \in K^n$ heißt *affine Abbildung*. Die Menge der affinen Abbildungen

$$\mathrm{Aff}_n(K) = \{f_{v,A}\colon K^n \to K^n \mid A \in \mathrm{GL}_n(K) \text{ und } v \in K^n\}$$

bildet mit der Verknüpfung von Abbildungen eine Untergruppe von $\mathrm{Sym}(K^n)$, denn

$$f_{v,A} \circ f_{w,B}(x) = v + A(w + Bx) = v + Aw + ABx = f_{Aw+v,AB}(x)$$

für alle $x \in K^n$ und die Umkehrabbildung von $f_{v,A}$ ist $f_{-A^{-1}v,A^{-1}}$. Die Gruppe $\mathrm{Aff}_n(K)$ heißt die *affine Gruppe* des K^n.

Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ ist eine Untergruppe von $\mathrm{Aff}_n(K)$; sie besteht genau aus den Abbildungen der Form $f_{0,A}$. Die affinen Abbildungen der

Form $T_v = f_{v,E_n}$ nennt man *Translationen*. Die Menge der Translationen

$$T(K^n) = \{T_v \mid v \in K^n\}$$

bildet ebenfalls eine Untergruppe der affinen Gruppe. (Übungsaufgabe: $T(K^n)$ ist isomorph zu $(K^n, +)$). Die Gruppe der Translationen ist ein Normalteiler **L**
von $\mathrm{Aff}_n(K)$, denn es gilt

$$f_{v,A} \circ T_w \circ f_{v,A}^{-1}(x) = v + A(w - A^{-1}v + A^{-1}x) = Aw + x = T_{Aw}(x)$$

für alle $x \in K^n$. Wir beobachten nun $f_{v,A} = T_v \circ f_{0,A}$, also gilt $\mathrm{Aff}_n(K) = T(K^n)\,\mathrm{GL}_n(K)$. Weil nur die Translation T_0 den Nullvektor fixiert, gilt auch $T(K^n) \cap \mathrm{GL}_n(K) = \{\mathrm{id}_{K^n}\}$. Nun folgt aus Satz 2.4.17, dass die affine Gruppe isomorph zum semidirekten Produkt

$$\mathrm{Aff}_n(K) \cong K^n \rtimes \mathrm{GL}_n(K)$$

ist. Die Wirkung von $\mathrm{GL}_n(K)$ auf K^n ist dabei die Wirkung aus Beispiel 2.1.5.

2.4.21 **Kurze exakte Folgen**. Es seien G, H und K Gruppen und $\alpha\colon K \to G$ und $\beta\colon G \to H$ Homomorphismen. Man nennt die *Folge*

$$K \xrightarrow{\alpha} G \xrightarrow{\beta} H$$

exakt bei G, wenn $\mathrm{Bild}(\alpha) = \mathrm{Ker}(\beta)$ gilt.

Zwei spezielle Fälle werden sehr häufig gebraucht. Nehmen wir zunächst an, dass $K = \{e\}$ die triviale Gruppe ist. Die Folge

$$\{e\} \longrightarrow G \xrightarrow{\beta} H$$

ist also genau dann exakt, wenn $\mathrm{Ker}(\beta) = \{e\}$ gilt, d.h., wenn β injektiv ist (1.2.10). Nun schauen wir uns den Fall an, dass $H = \{e\}$ die triviale Gruppe ist. Die Folge

$$K \xrightarrow{\alpha} G \longrightarrow \{e\}$$

ist genau dann exakt, wenn $\alpha(K) = G$ gilt, d.h., wenn α surjektiv ist.

Man bezeichnet

$$\{e\} \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \{e\}$$

als *kurze exakte Folge*, wenn die Folge bei K, G und H exakt ist. Es gilt also α ist injektiv, β ist surjektiv und $\mathrm{Bild}(\alpha) = \mathrm{Ker}(\beta)$. In diesem Fall ist $\alpha(K)$ ein zu K isomorpher Normalteiler von G und die Faktorgruppe $G/\alpha(K)$ ist isomorph zu H; siehe 1.3.11. Man nennt G dann eine *Erweiterung von K durch H*.

2.4.22 Aufgabe. Es sei G eine Erweiterung von K durch H. Zeigen Sie: Sind K und H endlich, dann ist auch G endlich und es gilt $|G| = |K| \cdot |H|$. **L**

2.4.23 Spaltende kurze exakte Folgen. Es sei

$$\{e\} \longrightarrow N \xrightarrow{j} G \xrightarrow{\beta} H \longrightarrow \{e\}$$

eine kurze exakte Folge von Gruppen. Man sagt, dass die Folge *spaltet*, wenn es einen Homomorphismus $s\colon H \to G$ gibt mit der Eigenschaft

$$\beta(s(h)) = h$$

für alle $h \in H$. Der Homomorphismus s ist also rechtsinvers zu β; man nennt s eine *Spaltabbildung*. Die Existenz einer Spaltabbildung kann man durch ein Diagramm der Form

$$\begin{tikzcd} \{e\} \arrow[r] & N \arrow[r, "j"] & G \arrow[r, "\beta"] & H \arrow[l, bend left, dotted, "s"] \arrow[r] & \{e\} \end{tikzcd}$$

darstellen. Eine Spaltabbildung ist übrigens immer injektiv, denn aus $s(h) = e$ folgt $h = \beta(s(h)) = e$.

2.4.24 Satz. *Ist*

$$\begin{tikzcd} \{e\} \arrow[r] & N \arrow[r, "j"] & G \arrow[r, "\beta"] & H \arrow[l, bend left, dotted, "s"] \arrow[r] & \{e\} \end{tikzcd}$$

eine spaltende kurze exakte Folge von Gruppen, dann ist G isomorph zu einem semidirekten Produkt $N \rtimes H$.

__Beweis.__ Da j injektiv ist, ist das Bild von j isomorph zu N. Um die Notation etwas zu vereinfachen, identifizieren wir N mit dem Bild $j(N)$ und tun so, als sei $N \subseteq G$ und j die Inklusionsabbildung.

Zuerst müssen wir eine Wirkung von H auf N finden. Dazu verwenden wir die Spaltabbildung und definieren

$$w(h,n) := {}^{s(h)}n = s(h)ns(h)^{-1}.$$

Nun verwenden wir wieder die universelle Eigenschaft des semidirekten Produktes für die Abbildungen $f_N = j$ und $f_H = s$ und erhalten einen Homomorphismus

$$\hat{f}\colon N \rtimes_w H \to G \quad \text{mit} \quad \hat{f}(n,h) = ns(h).$$

Wir müssen uns nun davon überzeugen, dass $\hat{f}$ ein Isomorphismus ist. Der Homomorphismus $\hat{f}$ ist surjektiv, denn für alle $g \in G$ gilt

$$g = (\underbrace{gs(\beta(g))^{-1}}_{\in N})s(\beta(g)) = \hat{f}(gs(\beta(g))^{-1}, \beta(g)).$$

Um zu sehen, dass $\hat{f}$ auch injektiv ist, nehmen wir ein Element (n,h) im Kern. Dann gilt $\hat{f}(n,h) = ns(h) = e$ und damit auch $s(h) \in N = \mathrm{Ker}(\beta)$. Daraus folgt nun $e = \beta(s(h)) = h$ und damit auch $n = e$. □

III. Die Isometriegruppe des $\mathbb{R}^n$

2.4.25 Die Isometriegruppe des $\mathbb{R}^n$. Am Ende dieses Abschnitts begeben wir uns auf eine kleine Exkursion und untersuchen die Isometriegruppe

$$\mathrm{Isom}(\mathbb{R}^n) = \{f\colon \mathbb{R}^n \to \mathbb{R}^n \mid d(f(u), f(v)) = d(u,v) \ \text{ für alle } u, v \in \mathbb{R}^n\ \}.$$

Wir werden sehen, dass sich die Isometriegruppe wieder als semidirektes Produkt verstehen lässt.

In Beispiel 1.1.13 hatten wir schon zwei Arten von Isometrien erwähnt:

- Die Translationen $T_w\colon x \mapsto x + w$ mit $w \in \mathbb{R}^n$ und
- die orthogonalen linearen Abbildungen $x \mapsto Ax$ mit $A \in \mathrm{O}(n)$.

Etwas allgemeiner erhält man durch Verknüpfung nun die Abbildungen

$$f_{w,A}\colon \mathbb{R}^n \to \mathbb{R}^n \quad \text{mit} \quad f_{w,A}(x) = w + Ax$$

mit einem Vektor $w \in \mathbb{R}^n$ und einer orthogonalen Matrix $A \in \mathrm{O}(n)$. Abbildungen dieser Art sind uns schon in Beispiel 2.4.20 begegnet. In der Tat ist $f_{w,A}$ eine Isometrie, denn für alle $u, v \in \mathbb{R}^n$ gilt

$$d(f_{w,A}(u), f_{w,A}(v)) = \|(w+Au)-(w+Av)\| = \|A(u-v)\| = \|u-v\| = d(u,v);$$

hier verwenden wir im vorletzten Schritt, dass A orthogonal ist. Wir wollen nun beweisen, dass jede des $\mathbb{R}^n$ Isometrie von der Form $f_{w,A}$ ist.

2.4.26 **Satz über die Isometriegruppe des $\mathbb{R}^n$.** *Die Elemente von* $\mathrm{Isom}(\mathbb{R}^n)$ *sind genau die Abbildungen der Form $f_{w,A}$ für einen Vektor $w \in \mathbb{R}^n$ und eine orthogonale Matrix $A \in \mathrm{O}(n)$. Insbesondere gibt es einen Isomorphismus*

$$\mathrm{Isom}(\mathbb{R}^n) \cong \mathbb{R}^n \rtimes \mathrm{O}(n)$$

wobei das semidirekte Produkt bezüglich der kanonischen Wirkung von $\mathrm{O}(n)$ *auf* $\mathbb{R}^n$ *gebildet wird.*

Beweis. Wir wissen bereits, dass die Abbildungen $f_{w,A}$ Isometrien sind. Zuerst wollen wir zeigen, dass Isometrien Geraden auf Geraden abbilden. Dazu benötigen wir etwas lineare Algebra.

Es seien $x, x' \in \mathbb{R}^n$ mit $x \neq x'$ gegeben. Die Gerade durch x und x' besteht genau aus den Punkten der Form $(1-t)x + tx'$ mit $t \in \mathbb{R}$. Es sei nun $\lambda \in \mathbb{R}$ fest gewählt. Wir zeigen: *Der Punkt $(1-\lambda)x + \lambda x'$ ist der eindeutige Punkt im $\mathbb{R}^n$, der von x den Abstand $|\lambda|\|x-x'\|$ und von x' den Abstand $|1-\lambda|\|x-x'\|$ hat.*

Dass $(1-\lambda)x + \lambda x'$ diese Eigenschaften besitzt ist klar, wir müssen uns aber überlegen, warum es keinen anderen solchen Punkt gibt. Es sei also $y \in \mathbb{R}^n$ ein Punkt mit diesen Eigenschaften, d.h.,

$$\begin{aligned} \lambda^2\|x-x'\|^2 &= \langle y-x, y-x\rangle = \|y\|^2 - 2\langle y, x\rangle + \|x\|^2 \\ (1-\lambda)^2\|x-x'\|^2 &= \langle y-x', y-x'\rangle = \|y\|^2 - 2\langle y, x'\rangle + \|x'\|^2. \end{aligned}$$

Subtrahieren wir die obere Zeile von der unteren und ziehen zusätzlich noch $\|x - x'\|^2$ ab, dann erhalten wir

$$-2\lambda\|x - x'\|^2 = 2\langle y - x, x - x'\rangle$$

Wir wollen zeigen, dass y auf der Gerade durch die Punkte x und x' liegt. Die Cauchy-Schwarz Ungleichung (siehe „Lineare Algebra" 6.1.9) liefert nun

$$|\lambda|\|x - x'\|^2 = |\langle y - x, x - x'\rangle| \overset{\star}{\leq} \|y - x\|\|x - x'\| = |\lambda|\|x - x'\|,$$

wobei im Schritt $\star$ nur dann Gleichheit besteht, wenn $y - x$ und $x - x'$ linear abhängig sind, d.h., wenn y auf der Gerade durch x und x' liegt. Daher muss y von der Form $y = (1-t)x + tx'$ sein für ein $t \in \mathbb{R}$. Da $|t| = |\lambda|$ und $|1-t| = |1-\lambda|$ gelten, muss $t = \lambda$ sein. Es sei nun $f \in \mathrm{Isom}(\mathbb{R}^n)$ beliebig. Weil f Abstände erhält, gilt nun also

$$f((1 - \lambda)x + \lambda x') = (1 - \lambda)f(x) + \lambda f(x') \tag{2.4.a}$$

für alle $x, x' \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$.

Als nächstes beweisen wir, dass f von der Form $f = f_{w,A}$ ist. In diesem Fall wäre $w = f(0)$, also definieren wir einfach $w := f(0)$. Wir untersuchen nun die Isometrie $f' = T_{-w} \circ f$. Diese erfüllt $f'(0) = 0$ und wenn die Aussage des Satzes richtig ist, dann ist f' eine orthogonale lineare Abbildung.

Aus 2.4.a folgt mit $x = 0$, dass f' homogen ist, d.h., für alle $x' \in \mathbb{R}^n$ und alle $\lambda \in \mathbb{R}$ gilt die Identität

$$f'(\lambda x') = \lambda f'(x').$$

Aus der Homogenität und Gleichung 2.4.a ergibt sich

$$f'(x + x') = 2f'(\frac{1}{2}(x + x')) = 2(\frac{1}{2}f(x) + \frac{1}{2}f(x')) = f(x) + f(x').$$

Die Abbildung f' ist also linear und weil f' Abstände erhält, handelt es sich um eine orthogonale Abbildung $f'(v) = Av$ mit $A \in \mathrm{O}(n)$; siehe „Lineare Algebra", Proposition 6.3.12.

Zuletzt wollen wir zeigen, dass $\mathrm{Isom}(\mathbb{R}^n)$ ein semidirektes Produkt ist. Das funktioniert genau wie in Beispiel 2.4.20. Dazu prüft man zunächst, dass die Menge der Translationen $T(\mathbb{R}^n) = \{T_w \mid w \in \mathbb{R}^n\}$ ein zu $\mathbb{R}^n$ isomorpher Normalteiler von $\mathrm{Isom}(\mathbb{R}^n)$ ist. Die Untergruppe der orthogonalen Abbildungen $f_{0,A}$ ist ein Komplement von $T(\mathbb{R}^n)$, deshalb sieht man mit Satz 2.4.17, dass $\mathrm{Isom}(\mathbb{R}^n)$ ein semidirektes Produkt der Form $\mathbb{R}^n \rtimes \mathrm{O}(n)$ ist. Um die Wirkung von $\mathrm{O}(n)$ auf $T(\mathbb{R}^n)$ auszurechnen, konjugieren wir eine Translation mit einer orthogonalen Abbildung:

$$f_{0,A} \circ T_w \circ f_{0,A}^{-1}(v) = A(w + A^{-1}v) = Aw + v = T_{Aw}(v). \qquad \square$$

2.6. Lösungen der Aufgaben in Kurseinheit 2

L2.1.9 **Lösung.** Es sei $z \in \mathcal{H}$ und

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

Wir betrachten die Möbius-Transformation

$$A \cdot z := \frac{az+b}{cz+d}.$$

Wir müssen zunächst prüfen, dass hier nicht durch Null dividiert wird. Falls der Nenner verschwindet, dann ist die Zahl cz reell. Weil aber $\Im(z) > 0$ gilt, ist die komplexe Zahl cz nur dann reell, wenn $c = 0$ ist. Aus $c = 0$ folgt aber stets $d \neq 0$, denn die Determinante $\det(A) = ad - bc$ ist 1.

Als nächstes überlegen wir uns, ob $A \cdot z$ wieder in $\mathcal{H}$ liegt. Dazu bestimmen wir den Imaginärteil. Es sei $z = x + yi$. Dann gilt

$$\frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{(acx^2 + adx + acy^2 + bcx + bd)}{|cz+d|^2} + \frac{(ad-bc)y}{|cz+d|^2} i$$

Wegen $\det(A) = ad - bc = 1$ ist der Imaginärteil von $A \cdot z$ genau $\frac{y}{|cz+d|^2}$ und ist damit positiv.

Die Möbius-Transformationen definieren eine Wirkung von $\mathrm{SL}_2(\mathbb{R})$ auf $\mathcal{H}$. Offensichtlich ist $E_2 \cdot z = z$. Es seien nun

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Dann gilt

$$AB = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix},$$

und damit

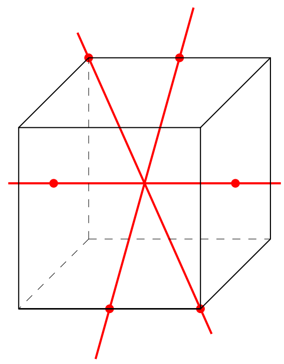
$$\begin{aligned} A \cdot (B \cdot z) &= A \cdot \left(\frac{a'z + b'}{c'z + d'} \right) = \frac{a \frac{a'z+b'}{c'z+d'} + b}{c \frac{a'z+b'}{c'z+d'} + d} \\ &= \frac{aa'z + ab' + b(c'z + d')}{ca'z + cb' + d(c'z + d')} = \frac{(aa' + bc')z + ab' + bd'}{(ca' + dc')z + cb' + dd'} = (AB) \cdot z. \end{aligned}$$

L2.1.24 **Lösung.** (1): Die Drehgruppe $D(W)$ wirkt transitiv auf der Menge der 6 Seitenflächen des Würfels. Die Bahnengleichung 2.1.21 ermöglicht es uns, die Ordnung der Drehgruppe $D(W)$ zu bestimmen, indem wir die Ordnung der Stabilisatorgruppe bestimmen.

Welche Drehungen des Würfels stabilisieren eine vorgegebene Seite $S \subseteq W$? Wenn eine Drehung f die Seite S stabilisiert, d.h, $f(S) = S$, dann stabilisiert f auch die gegenüberliegende Seite und die Mittelpunkte dieser beiden Seiten. Es kann sich also nur um eine Drehung um die Achse durch die beiden gegenüberliegenden Seitenmittelpunkte handeln. Davon gibt es 4 Stück: die Drehungen um $0°$, $90°$, $180°$ und $270°$. Also gilt $|\,\mathrm{St}_{D(W)}(S)| = 4$ und mit der Bahnengleichung erhalten wir

$$|D(W)| = |D(W) \cdot S| \cdot |\,\mathrm{St}_{D(W)}(S)| = 6 \cdot 4 = 24.$$

Man kann nun mit etwas rumprobieren alle Drehungen auflisten. Die 24 Elemente der Drehgruppe sind:



(a) Die Identität (Anzahl: 1).

(b) Drehungen um $180°$ Grad um die Achse durch zwei gegenüberliegende Seitenmittelpunkte (Anzahl: 3).

(c) Drehungen um $90°$ oder $270°$ Grad um die Achse durch zwei gegenüberliegende Seitenmittelpunkte (Anzahl: $3 \cdot 2 = 6$).

(d) Drehungen um $180°$ um die Achse durch zwei gegenüberliegender Kantenmittelpunkte (Anzahl: 6).

(e) Drehungen um 120° oder 240° Grad um die Achse
durch zwei diametral gegenüberliegende Ecken (Anzahl: $4 \cdot 2 = 8$).

(2): Wir wollen das Abzählproblem mithilfe der Burnside'schen Formel 2.1.22 lösen. Dazu sei X die Menge aller schwarz-weiß gefärbter Würfel. Die Menge X enthält $2^6 = 64$ Elemente. Die Drehgruppe $D(W)$ wirkt auf X durch Drehungen und wir wollen genau die Anzahl der Bahnen bestimmen. Dazu müssen wir für jedes Element der Drehgruppe, die Anzahl der fixierten Färbungen bestimmen. Dazu verwenden wir die Liste aus Teil (1).

(a) Die Identität fixiert jede Färbung, d.h, $|\operatorname{Fix}_X(\mathrm{id})| = 64$.

(b) Die Drehungen um 180° Grad um die Achse durch zwei gegenüberliegende Seitenmittelpunkte fixieren jeweils $2^4 = 16$ Färbungen.

(c) Die Drehungen um 90° oder 270° Grad um die Achse durch zwei gegenüberliegende Seitenmittelpunkte fixieren jeweils $2^3 = 8$ verschiedene Färbungen.

(d) Die Drehungen um 180° um die Achse durch zwei gegenüberliegender Kantenmittelpunkte fixieren jeweils $2^3 = 8$ verschiedene Färbungen.

(e) Drehungen um 120° oder 240° Grad um die Achse durch zwei diametral gegenüberliegende Ecken fixieren jeweils $2^2 = 4$ verschiedene Färbungen.

Mit der Burnside'schen Formel 2.1.22 erhalten wir

$$|X/D(W)| = \frac{1}{24}(64 + 3 \cdot 16 + 6 \cdot 8 + 6 \cdot 8 + 8 \cdot 4) = 10.$$

Es gibt also 10 verschiedene schwarz-weiß Färbungen des Würfels.

L2.2.7 **Lösung.** Wir wollen zeigen, dass

$$M = \{\sigma \in S_n \mid \sigma(n) = n\} = \operatorname{St}_{S_n}(n)$$

eine maximale Untergruppe von S_n ist. Dazu sei $\tau \in S_n \setminus M$ beliebig, d.h. $\tau(n) \neq n$. Wir zeigen, dass $\langle M \cup \{\tau\}\rangle = S_n$ gilt; vgl. 2.2.4. Sagen wir $\tau(n) = i < n$. Es sei nun $\pi \in S_n$ beliebig. Wir wollen $\pi \in \langle M \cup \{\tau\}\rangle$ beweisen. Falls $\pi \in M$

liegt, ist nichts zu tun. Also nehmen wir $\pi \notin M$ an; es gilt also $\pi(n) = j < n$. Die Transposition $(i\ \ j)$ liegt in M und es gilt

$$\tau^{-1} \circ (i\ \ j) \circ \pi(n) = \tau^{-1}(i) = n,$$

d.h., $\mu := \tau^{-1}(i\ \ j)\pi \in M$. Wir schließen daraus $\pi = (i\ \ j)\tau\mu \in \langle M \cup \{\tau\}\rangle$.

L2.2.20 Lösung. Es sei $k \geq 1$. Gegeben sind zwei k-Tupel $(m_1, \ldots, m_k), (m'_1, \ldots, m'_k) \in \mathbb{N}^{[k]}$ mit paarweise verschiedenen Einträgen. Wir wählen $n \in \mathbb{N}$ größer als alle vorkommenden Einträge $m_1, \ldots, m_k, m'_1, \ldots, m'_k$. Insbesondere ist $n > k$. Da die Gruppe S_n bereits n-transitiv (und damit auch k-transitiv auf $\{1, \ldots, n\}$ wirkt (siehe 2.2.19), finden wir eine Permuatition $\sigma \in S_n$ mit $\sigma(m_i) = m'_i$ für alle $i \in \{1, \ldots, k\}$. Wir definieren nun $\hat{\sigma} \in \mathrm{Sym}(\mathbb{N})$ durch

$$\hat{\sigma}(x) = \begin{cases} \sigma(x) & \text{falls } x \leq n \\ x & \text{falls } x > n \end{cases}$$

und stellen fest, dass $\hat{\sigma}(m_i) = m'_i$ für alle $i \in \{1, \ldots, k\}$ gilt.

L2.2.24 Lösung. Wir beobachten zuerst, dass die alternierende Gruppe A_n für $n \geq 3$ transitiv auf $\{1, 2, \ldots, n\}$ wirkt. In der Tat, sind $i \neq j$ beliebigm dann gibt es wegen $n \geq 3$ ein Element $k \in \{1, \ldots, n\} \setminus \{i, j\}$. Der 3-Zykel $(i\ \ j\ \ k) \in A_n$ bildet i auf j ab.

Es sei nun $n \geq 4$. Der Stabilisator $\mathrm{St}_{A_n}(i)$ enthält eine zu A_{n-1} isomorphe Untergruppe, die von den 3-Zykeln auf $\{1, 2, \ldots, n\} \setminus \{i\}$ erzeugt wird. Da diese Wirkung transitiv ist, folgt die Behauptung aus 2.2.22.

L2.3.3 Lösung. Es seien $g_i, h_i, k_i \in G_i$. Assoziativität:

$$\begin{aligned}\big((g_i)_{i\in I}(h_i)_{i\in I}\big)(k_i)_{i\in I} &= (g_ih_i)_{i\in I}(k_i)_{i\in I} = ((g_ih_i)k_i)_{i\in I} = (g_i(h_ik_i))_{i\in I} \\ &= (g_i)_{i\in I}(h_ik_i)_{i\in I} = (g_i)_{i\in I}\big((h_i)_{i\in I}(k_i)_{i\in I}\big)\end{aligned}$$

Neutrales Element:

$$(e_{G_i})_{i\in I}(g_i)_{i\in I} = (e_{G_i}g_i)_{i\in I} = (g_i)_{i\in I}$$

Inverse:

$$(g_i^{-1})_{i\in I}(g_i)_{i\in I} = (g_i^{-1}g_i)_{i\in I} = (e_{G_i})_{i\in I}$$

Wir verwenden hier, dass es ausreichend ist die Existenz von links-neutralem und links-inversen Elementen nachzuweisen; vgl. 1.1.3.

L2.3.5 **Lösung.** Es seien $h, k \in H$. Dann zeigt folgende Rechnung, dass $\Pi\alpha$ ein Homomorphismus ist:

$$\begin{aligned}\Pi\alpha(hk) &= (\alpha_i(hk))_{i\in I} = (\alpha_i(h)\alpha_i(k))_{i\in I}\\ &= (\alpha_i(h))_{i\in I}(\alpha_i(k))_{i\in I} = \Pi\alpha(h)\Pi\alpha(k)\end{aligned}$$

Dabei verwendet man die Voraussetzung, dass alle α_i Homomorphismen sind.

L2.3.8 **Lösung.** Es seien nun N_1, N_2, N_3 drei Normalteiler von G. Zunächst nehmen wir an, dass $N_i \cap N_j = \{e\}$ für alle $i \neq j$ gilt (wir werden bald feststellen, dass diese Bedingung nicht ausreicht!). In diesem Fall kommutieren die Elemente von N_i und N_j paarweise; siehe 2.3.6. Wir erhalten also wieder eine Abbildung

$$p\colon N_1 \times N_2 \times N_3 \to G \quad \text{mit} \quad (n_1, n_2, n_3) \mapsto n_1n_2n_3$$

die (genau wie in 2.3.7) ein Gruppenhomomorphismus ist.

Jetzt bestimmen wir den Kern von p. Es sei $(n_1, n_2, n_3) \in \mathrm{Ker}(p)$. Angenommen (n_1, n_2, n_3) ist nicht trivial, dann ist $n_1 \neq e$, $n_2 \neq e$ und $n_3 \neq e$. Dann gilt $n_1n_2n_3 = e$ und somit insbesondere $n_1 = n_3^{-1}n_2^{-1} = n_2^{-1}n_3^{-1} \in N_2N_3$. Sei umgekehrt $m_1 \in N_1 \cap N_2N_3$, d.h., $m_1 = m_2m_3$ mit $m_2 \in N_2$ und $m_3 \in N_3$. Dann liegt $(m_1, m_2^{-1}, m_3^{-1})$ im Kern von p. Weil $N_2 \cap N_3 = \{e\}$ ist, ist der Kern von p also genau dann trivial, wenn $N_1 \cap N_2N_3 = \{e\}$ gilt.

Nun machen wir noch eine kleine Beobachtung: Aus $N_1 \cap N_2N_3 = \{e\}$ folgt bereits $N_1 \cap N_2 = \{e\}$ und $N_1 \cap N_3 = \{e\}$, denn $N_2, N_3 \subseteq N_2N_3$. Deshalb bietet sich folgende Verallgemeinerung von 2.3.7 an.

Sind N_1, N_2, N_3 Normalteiler von G und gilt $N_1 \cap N_2N_3 = N_2 \cap N_3 = \{e\}$, dann ist die Abbildung $p\colon N_1 \times N_2 \times N_3 \to G$ mit $(n_1, n_2, n_3) \mapsto n_1n_2n_3$ ein injektiver Homomorphismus von Gruppen. Falls zusätzlich $N_1N_2N_3 = G$ gilt, dann ist p ein Isomorphismus.

L2.3.15 Lösung. Wir wollen zeigen, dass

$$\beta(g) = \prod_{i \in S(g)} \alpha_i(g_i)$$

einen Homomorphismus definiert. Natürlich kann man in der Definition von β das Produkt auch über eine größere endliche Indexmenge laufen lassen, denn für alle $i \notin S(g)$ gilt $g_i = e$ und somit $\alpha_i(g_i) = e$. Es seien $g = (g_i)_{i \in I}, h = (h_i)_{i \in I} \in \prod'_{i \in I} G_i$. Offensichtlich gilt $S(gh) \subseteq S(g) \cup S(h)$. Damit erhält man

$$\begin{aligned} \beta(gh) = \prod_{i \in S(g) \cup S(h)} \alpha_i(g_i h_i) &= \prod_{i \in S(g) \cup S(h)} \alpha_i(g_i)\alpha_i(h_i) \\ &= \prod_{i \in S(g)} \alpha_i(g_i) \prod_{i \in S(h)} \alpha_i(h_i) = \beta(g)\beta(h). \end{aligned}$$

L2.3.16 Lösung. Es seien $g = (g_i)_{i \in I} \in \prod'_{i \in I} G_i$ und $h = (h_i) \in \prod_{i \in I} G_i$. Für fast alle $i \in I$ gilt $g_i = e$ und damit $h_i g_i h_i^{-1} = e$. Daher ist $hgh^{-1} \in \prod'_{i \in I} G_i$ und somit ist $\prod'_{i \in I} G_i$ ein Normalteiler; siehe 1.2.24.

L2.4.11 Lösung. (a): Um zu zeigen, dass D_∞ von zwei Elementen der Ordnung 2 erzeugt wird, gehen wir genauso vor wie bei den endlichen Diedergruppen. Die Elemente $r = (1, 1)$ und $s = (0, -1)$ erzeugen D_∞, denn $(k, -1) = r^k s$ und $(k, 1) = r^k$ für alle $k \in \mathbb{Z}$. Dabei ist s ein Element der Ordnung 2, aber r ein Element unendlicher Ordnung. Weiter gilt die Relation $srs = r^{-1}$ (nachrechnen!). Wir definieren $t = rs$ und stellen fest, dass t ein Element der Ordnung 2 ist:

$$t^2 = rsrs = rr^{-1} = e.$$

Wegen $r = ts$ gilt auch $D_\infty = \langle s, t \rangle$.

(b) Für jedes $n \geq 2$ ist die Abbildung

$$\rho_n \colon D_\infty \to D_{2n} \quad \text{mit} \quad \rho_n(k, \delta) = (k + n\mathbb{Z}, \delta)$$

ein Gruppenhomomorphismus, denn es gilt

$$\rho_n((k,\delta)(k',\delta')) = \rho_n(k+\delta k', \delta\delta') = (k+\delta k' + n\mathbb{Z}, \delta\delta')$$
$$= (k+n\mathbb{Z},\delta)(k'+n\mathbb{Z},\delta') = \rho_n(k,\delta)\rho_n(k',\delta').$$

Da ρ_n offensichtlich surjektiv ist, schließen wir mit 1.3.11, dass $D_{2n} \cong D_\infty/\mathrm{Ker}(\rho_n)$ gilt.

L2.4.13 Lösung. (a): Wir bestimmen zunächst die Automorphismengruppe von $\mathbb{Z}$. Aus 1.4.2 wissen wir bereits, dass nur die Elemente 1 oder -1 die zyklische Gruppe $\mathbb{Z}$ erzeugen. Sei nun $\alpha \in \mathrm{Aut}(\mathbb{Z})$. Mit Hilfssatz 1.4.8 sieht man nun, dass entweder $\alpha(1) = 1$ oder $\alpha(1) = -1$ gilt. Im ersten Fall ist α die Identität, im zweiten Fall die Inversion; hier verwenden wir 1.4.8 (ii). Es ist also $\mathrm{Aut}(\mathbb{Z}) \cong \{\pm 1\}$ und das nicht-triviale Element von $\mathrm{Aut}(\mathbb{Z})$ wirkt durch Inversion auf $\mathbb{Z}$. Damit erhält man $\mathrm{Hol}(\mathbb{Z}) \cong D_\infty$.

(b): Die Automorphimengruppe von $\mathbb{Z}/m\mathbb{Z}$ hat genau $\varphi(m)$ viele Elemente; siehe 1.5.9. Damit ergibt sich

$$|\,\mathrm{Hol}(\mathbb{Z}/m\mathbb{Z})| = |\mathbb{Z}/m\mathbb{Z}| \cdot |\,\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})| = m\varphi(m).$$

L2.4.20 Lösung. Um zu sehen, dass die Translationsgruppe $T(K^n)$ isomorph zu K^n ist, betrachten wir die Abbildung

$$T\colon K^n \to T(K^n)$$

mit $t\colon v \mapsto t_v$. Dies ist ein Gruppenhomomorphismus, denn

$$T_{v+w} = T_v \circ T_w$$

für alle $v, w \in K^n$. Offensichtlich ist die Abbildung t bijektiv, also handelt es sich um einen Isomorphismus.

L2.4.22 Lösung. Es sei G eine Erweiterung endlicher Gruppen K, H, d.h., es gibt eine kurze exakte Folge

$$\{e\} \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \{e\}.$$

Literaturverzeichnis

[Bau61] Gilbert Baumslag. Wreath products and finitely presented groups. *Math. Z.*, 75:22–28, 1960/61.

[BH99] Martin R. Bridson and André Haefliger. *Metric spaces of non-positive curvature*, volume 319 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[BS62] G. Baumslag and D. Solitar. Some two-generator one-relator non-Hopfian groups. *Bull. Am. Math. Soc.*, 68:199–201, 1962.

[Bur02] W. Burnside. On an unsettled question in the theory of discontinuous groups. *Quart. J.*, 33:230–238, 1902.

[Deh11] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71:116–144, 1911.

[Dei14] A. Deitmar. *Analysis.* Springer-Lehrbuch. Springer-Verlag, Berlin, 2014.

[Fis17] G. Fischer. *Lehrbuch der Algebra.* Springer-Lehrbuch. Springer-Verlag, Berlin, 2017. 4. Auflage.

[For17] O. Forster. *Analysis 2.* Springer-Lehrbuch. Springer-Verlag, Berlin, 2017. 11. Auflage.

[Fro87] G. Frobenius. Ueber die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul. *J. Reine Angew. Math.*, 101:273–299, 1887.

[Gro93] M. Gromov. Asymptotic invariants of infinite groups. In *Geometric group theory, Vol. 2 (Sussex, 1991)*, volume 182 of *London Math. Soc.*

Lecture Note Ser., pages 1–295. Cambridge Univ. Press, Cambridge, 1993.

[HNN49] G. Higman, B.H. Neumann, and H. Neumann. Embedding theorems for groups. *J. London Math. Soc.*, 24:247–254, 1949.

[JS14] J. C. Jantzen and J. Schwermer. *Algebra, 2. Auflage*. Springer-Lehrbuch. Springer-Verlag, Berlin, 2014.

[KM17] Ch. Karpfinger and K. Meyberg. *Algebra, 4. Auflage*. Springer-Lehrbuch. Springer Spektrum, 2017.

[Lan02] S. Lang. *Algebra*. uni-text. Springer-Verlag, New York, 2002.

[Led77] Walter Ledermann. *Einführung in die Gruppentheorie*. uni-text. Vieweg & Sohn, Braunschweig, 1977.

[Löh17] Clara Löh. *Geometric Group Theory*. Springer International Publishing AG, 2017.

[LS01] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[Lys96] I. G. Lysënok. Infinite Burnside groups of even period. *Izv. Ross. Akad. Nauk Ser. Mat.*, 60(3):3–224, 1996.

[Mac12] Antonio Machi. *Groups*. Unitext. Springer-Verlag, Milan, 2012.

[Mes72] Stephen Meskin. Nonresidually finite one-relator groups. *Trans. Am. Math. Soc.*, 164:105–114, 1972.

[Nov55] P. S. Novikov. Über die algorithmische Unentscheidbarkeit des Wortproblems in der Gruppentheorie. Tr. Mat. Inst. Steklova 44, 140 S. (1955)., 1955.

[Rob95] Derek J. S. Robinson. *A course in the theory of groups. 2nd ed.*, volume 80. New York, NY: Springer-Verlag, 2nd ed. edition, 1995.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[Sch27] Otto Schreier. Die Untergruppen der freien Gruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:161–183, 1927.

[Ser80] Jean-Pierre Serre. *Trees*. Springer-Verlag, Berlin, 1980.

[Thé97] Jacques Thévenaz. Maximal subgroups of direct products. *J. Algebra*, 198(2):352–361, 1997.

Index